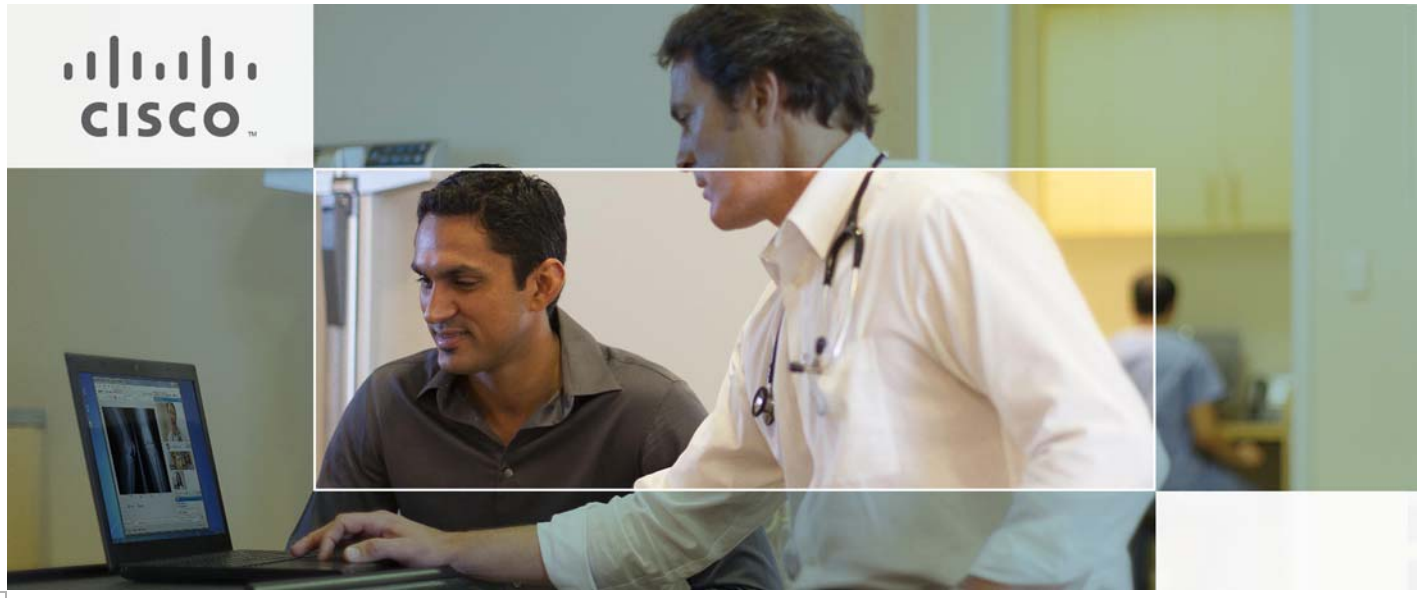


Cisco Compliance Solution for HIPAA Security Rule Design and Implementation Guide

A Cisco Validated Design

Cisco Validated Design

Solution Authors

Christian Janoff

Bart McGlothin

Christian Janoff, Compliance Solutions Architect, STBU, Cisco Systems

Christian Janoff is a Solution Architect at Cisco Systems with over 15 years of solution architecture and design experience. Christian leads Cisco's participation on the Payment Card Industry Security Standards Council. He was elected to the PCI Council's Board of Advisors in May, 2009. Prior to Cisco, Christian worked as a network engineering manager at Safeway, Inc. Christian holds a bachelor's degree from University of California at Santa Cruz.

Bart McGlothin, Compliance Solutions Architect, STBU, Cisco Systems

Bart McGlothin is a Solution Architect in the Compliance Solutions group at Cisco Systems, Inc. Bart leads the technical aspect of Cisco's Security framework for Compliance and more specifically; Payment Card Industry (PCI) initiatives including Cisco's Validated Designs for PCI compliance. He has over sixteen years of solution architecture and design experience. Bart leads Cisco's involvement with the National Retail Federation's Association for Retail Technology Standards Committee (ARTS) as a member of the ARTS board and Executive Committee. Prior to Cisco, Bart worked as the Network Architect at Safeway, Inc.

Partner Authors

Kenneth Luberto	Aaron Reynolds

Contributors

Mike Adler	Tom Hua
Mark Allen	Raymond Jett
Annette Blum	Manny Kamer
Renata Budko	Rekha Krishna
John Carney	Paul Lysander
Danny Dhillon	Fernando Macias
Michael Dugan	Bob Nusbaum
Zeeshan Farees	Manu Parbhakar
Carol Ferrara-Zarb	Vikram Prabhakar
Syed Ghayer	Jim Rintoul
Sujit Ghosh	Brian Robertson
Manisha Gupta	Angel Shimelish
Jamey Heary	Rick Simon
Gary Halleen	Maria Sisiruca
Stuart Higgins	Sheri Spence
Amanda Holdan	Greg Varga
Rob McIndoe	Terri Quinn

Preface

The assessments in the *Cisco Compliance Solution for HIPAA Security Rule Design and Implementation Guide* are based on the components assessed in the previous *Cisco Compliance Solution for PCI DSS 2.0 Design and Implementation Guide*. Therefore, some of these components may not be current.

CONTENTS

CHAPTER 1 **Solution Overview** 1-1

Introduction 1-1

Solution Methodology 1-2

Target Market/Audience 1-2

Solution Benefits 1-3

HIPAA Solution Summary Results 1-3

CHAPTER 2 **HIPAA and the Solution Framework** 2-1

Safeguard Applicability and Exclusions 2-2

Industry Standards 2-3

Control Mapping to the Cisco Reference Architecture 2-3

HIPAA Solution Framework 2-3

Endpoints/Applications 2-4

Administration 2-4

Infrastructure 2-5

Services 2-5

CHAPTER 3 **Solution Architecture** 3-1

Enterprise Architecture and HIPAA Design Considerations 3-2

Hospital and Clinic Architectures 3-4

Design Considerations 3-4

Data Center 3-9

Design Considerations 3-10

WAN Aggregation 3-12

Design Considerations 3-12

Core Layer 3-14

Design Considerations 3-14

Aggregation Block 3-15

Design Considerations 3-15

E-commerce/Internet Edge/Service Provider Edge/Partner Edge 3-18

Design Considerations 3-18

CHAPTER 4 **Solution Implementation** 4-1

Overview 4-1

Infrastructure 4-2

Healthcare Facilities—Clinics and Hospitals 4-5

Data Center 4-19

Administration 4-26

Authentication 4-26

PHI Encryption 4-26

Management 4-27

Monitoring 4-27

Endpoints and Applications 4-28

Physical 4-28

Voice 4-28

Services 4-29

Cisco Compliance Solution for HIPAA Security Rule Result Summary 4-30

CHAPTER 5 **Component Assessment** 5-1

Component Section Overview 5-1

Description 5-1

Assessment Summary 5-1

Primary Function 5-2

Design Considerations 5-2

Assessment Details 5-2

Endpoints 5-3

Voice 5-3

Physical Security 5-12

Administration 5-51

Authentication 5-51

Management 5-72

Encryption 5-87

Storage 5-92

Monitoring 5-99

Infrastructure 5-109

Routing 5-109

Switching 5-126

Wireless 5-146

Storage 5-157

Security 5-162

Intrusion Detection 5-179

CHAPTER 6 **Summary** 6-1

HIPAA Solution Summary Results 6-1

Lessons Learned 6-2

APPENDIX A **Bill Of Material** A-1

Managed Service Provider Clinic A-1

Doctor's Office A-4

Mini Clinic A-5

Small Clinic A-7

Medium Clinic A-10

Hospital A-14

Data Center, Internet Edge, DMZ A-19

Data Center—WAN Aggregation A-26

Data Center—Service A-28

Data Center—Secure Storage A-32

Data Center—Extranet Edge A-33

Data Center—Physical Security A-36

Data Center—Wireless Systems A-38

Data Center—Management A-39

Data Center—Access, Aggregation A-41

Data Center—UCS A-43

Data Center—Core A-45

APPENDIX B **Cisco Products and Software Versions** B-1

APPENDIX C **Reference Architecture Assessment Report—Cisco Healthcare Solution** C-1

Contact Information C-1

Table of Contents C-2

1. Executive Summary C-2

2. Introduction C-5

Reference Documentation C-5

Business Associate C-6

Timeframe C-6

Cisco's Healthcare Reference Architecture C-7

Reference Model Components C-8
Network Segmentation and Management C-9
Wireless LANs and/or Wireless Applications C-9
3. Assessment Findings and Conclusions C-10
3.1 Safeguard Exclusions C-10
3.2 Safeguards Provided throughout the Reference Model C-16
4. Safeguard Mapping to Security Control Areas C-18
5. Control Mapping to Cisco's Healthcare Reference Architecture C-24
6. Application of the Healthcare Reference Architecture C-26
7. Appendix C-28
Healthcare Security Requirements C-28
List of Interviews C-30
List of Documents C-31

APPENDIX D **Simplified Crosswalk—HIPAA, PCI, and SOX** D-1

APPENDIX E **Detailed Full Running Configurations** E-3
Table of Contents E-3
Data Center E-5
WAN E-5
Core E-37
Aggregation E-55
Access E-134
Storage E-175
Internet Edge E-199
WAN E-199
Converged Core/Aggregation E-215
Clinic E-254
Hospital E-254
Medium Clinic E-366
Small Clinic E-448
Mini Clinic E-489
Doctor's Office E-529
Managed Service Provider E-565

CHAPTER 1

Solution Overview

Introduction

Cisco customers have stated that the Health Insurance Portability and Accounting Act (HIPAA) is vague, and they are not sure how it directly applies to their enterprise networks. Many do not understand how HIPAA relates to technology and infrastructure. They have asked Cisco to provide guidance that shows this relationship. This Cisco Compliance Solution for HIPAA Security Rule provides a reference architecture designed to help covered entities and business associates simplify compliance with the HIPAA Security Rule. The guidance in this document maps architectures and products to the HIPAA Security Rule technical safeguards, standards, and implementation specifications.

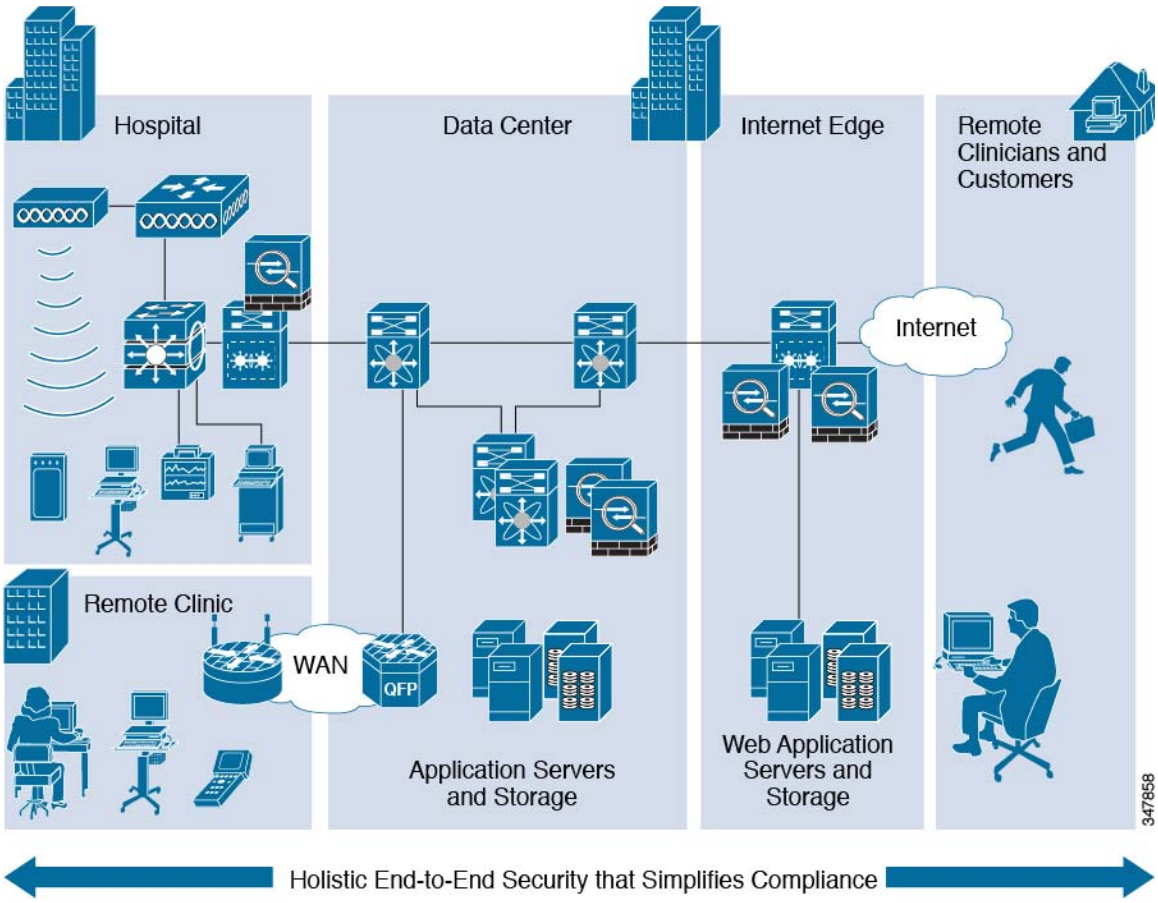
Chapter 2, "HIPAA and the Solution Framework," describes the elements that make up the solution framework. The solution framework organizes the scope of the Protected Health Information (PHI) data environment for contextual reference. Chapter 3, "Solution Architecture," discusses what IT should consider when designing their network to best align with HIPAA Security Rule implementation specifications. For specific designs referencing these architectures, read Chapter 4, "Solution Implementation." In Chapter 5, "Component Assessment," each component is individually assessed for its capabilities, and configuration examples are given to demonstrate this utility. The complete assessment report authored by Verizon is located in Appendix C, "Reference Architecture Assessment Report—Cisco Healthcare Solution."

The Cisco Compliance Solution for HIPAA Security Rule was built and tested using a holistic enterprise perspective including the following:

- Endpoint consideration—PHI systems and devices, including wireless devices
- Administrative concerns within scope of HIPAA
- Cisco, RSA, EMC, and Hytrust network infrastructure and architectures comprising data center, Internet edge, and healthcare facilities that simplify the process of meeting the HIPAA Security Rule implementation specifications.

Figure 1-1 shows an example of the enterprise architecture.

Figure 1-1 Enterprise Architecture



Solution Methodology

Cisco customers have asked for clarification on how HIPAA relates to Cisco architectures and individual components within the architecture. To address this challenge, Cisco contracted Verizon Business to "reassess" an existing compliance solution that protects credit card data; Cisco Compliance Solution for PCI DSS 2.0. The strategy is to use a common control structure that addresses multiple compliance standards using a "unified compliance" mindset. The intent is that regardless of the type of sensitive electronic data (payment or healthcare), a single security strategy should meet the needs of an organization to protect it from a compliance perspective.

Target Market/Audience

The audience for this solution includes compliance managers, as well as technical teams seeking guidance on how to design, configure, and maintain their IT architecture and components for HIPAA Security Rule compliance. Although the diagrams and references relate to healthcare institutions, the reference architecture also applies for other covered entities and business associate networks in relation to the HIPAA Security Rule.

Solution Benefits

The solution demonstrates how to design end-to-end enterprise systems that conform to the HIPAA Security Rule safeguards and provides the following benefits:

- Insight into the Cisco enterprise architecture and the controls used to address HIPAA Security Rule technical safeguards
- A detailed analysis and mapping of Cisco and partner components and their relationship with HIPAA Security Rule controls
- A scalable set of reference designs that can be used to establish the security controls necessary to achieve compliance with the HIPAA Security Rule
- A centralized management "tool kit" simplifying the operational challenges of an enterprise network
- The central focus of this design guide is the implementation of an architecture that meets the HIPAA safeguards; in addition, using the recommended segmentation strategies and additional quality of service (QoS) parameters can increase performance.

HIPAA Solution Summary Results

Table 1-1 lists the HIPAA citations that were addressed within the solution.

Table 1-1 HIPAA Citations Addressed

Citation	Title
164.308(a)(1)(i)	Security Management Process
164.308(a)(1)(ii)(D)	Information System Activity Review
164.308(a)(3)(ii)(A)	Authorization and/or Supervision
164.308(a)(3)(ii)(C)	Termination Procedures
164.308(a)(4)(ii)(A)	Isolating Health Care Clearinghouse Function
164.308(a)(4)(ii)(B)	Access Authorization
164.308(a)(4)(ii)(C)	Access Establishment and Modification
164.308(a)(5)(ii)(B)	Protection from Malicious Software
164.308(a)(5)(ii)(C)	Log-in Monitoring
164.308(a)(5)(ii)(D)	Password Management
164.308(a)(6)(ii)	Response and Reporting
164.308(a)(7)(i)	Contingency Plan
164.308(a)(8)	Evaluation
164.310(a)(2)(iii)	Facility Access Control and Validation Procedures
164.312(a)(2)(i)	Unique User Identification
164.312(a)(2)(ii)	Emergency Access Procedure
164.312(a)(2)(iii)	Automatic Logoff
164.312(a)(2)(iv)	Encryption and Decryption
164.312(b)	Audit Controls

Table 1-1 HIPAA Citations Addressed

164.312(c)(1)	Data Integrity
164.312(d)	Person or Entity Authentication
164.312(e)(2)(i)	Transmission Integrity Controls
164.312(e)(2)(ii)	Transmission Encryption

Compliance with the HIPAA Security Rule was assessed by an external auditor, Verizon Global Services Group.

Note This document does not guarantee compliance with the HIPAA Security Rule.

CHAPTER 2

HIPAA and the Solution Framework

The Health Insurance Portability and Accounting Act (HIPAA) was signed into law in 1996 (Public Law 104-191). The HIPAA Omnibus Final Rule was released January 2013, and included updates from the Health Information Technology for Economic and Clinical Health (HITECH) Act, breach notification, penalty tiers, and extended HIPAA compliance obligations to include both covered entities and business associates. Covered entities and business associates that create, receive, transmit, or maintain protected health information (PHI) in electronic form must make a good faith effort to protect the corporate computing environment from reasonably anticipated threats and vulnerabilities; and take reasonable and appropriate measures to protect the integrity, confidentiality, and security of such electronic data.

The HIPAA Omnibus Final Rule consists of three main parts (sections) that put in place security and privacy requirements for the protection of PHI:

- Part 160—General Administrative Requirements. Deals mostly with the legal, compliance, and penalty aspects of HIPAA
- Part 162—Administrative Requirements. Deals with unique identifiers for covered entities in healthcare, provisions for transactions, and many other administrative issues in healthcare
- Part 164—Security and Privacy. Deals with the safeguards for protecting PHI in electronic and paper media. Part 164 consists of the following:
  - Subpart A—General Provisions §164.1xx
  - Subpart B—Reserved
  - Subpart C—Security Standards for the Protection of Electronic Protected Health Information §164.3xx
  - Subpart D—Notification in Case of Breach of Unsecured Protected Health Information §164.4xx
  - Subpart E—Privacy of Individually Identifiable Health Information §164.5xx

  The Cisco solution described in this document relates primarily to Part 164 Security and Privacy Subpart C.

The HIPAA Security Rule requires covered entities and business associates to perform an analysis of the potential risks to the electronic PHI for which they are responsible; and to then develop, implement, and maintain appropriate security measures to safeguard the integrity, confidentiality, and availability of that data. The HIPAA Security Rule incorporates recognized security objectives and protections, but is intentionally technology-neutral. It provides standards and, in some cases, implementation specifications with which covered entities and business associates must comply. The scope and nature

of HIPAA compliance activities for each covered entity or business associate vary according to the specific environment and associated vulnerabilities as determined through risk assessment. Although the standard is objective, a covered entity or business associate's specific security controls may vary, because the HIPAA Omnibus Final Rule permits flexibility in the approach to compliance.

Cisco and Verizon have provided clarity to the HIPAA Security Rule by providing a reference use case common to an enterprise. This use case identifies specific risks as well as the appropriate technology and configurations that can be used to satisfy the respective controls for these risks. Combining Cisco's technology portfolio, reference architectures, and Verizon's HIPAA assessment expertise, Cisco customers can benefit from using this document as an illustrative example of how to apply the same technology, configurations, and architectures within their own organizations to satisfy the security safeguards of HIPAA.

Safeguard Applicability and Exclusions

HIPAA Part 164 Subpart C is made up of nine sections. Three of the sections are administrative and are not part of this assessment. The remaining six sections (Security Standards: General Rules; Administrative Safeguards; Physical Safeguards; Technical Safeguards; Organizational Requirements; and Policies and Procedures and Documentation Requirements) consist of 52 security safeguards. Verizon performed an initial assessment to determine whether the safeguards could be met by using specific technology components provided by Cisco.

Of the 52 safeguards in the current healthcare requirements, Verizon identified 29 safeguards as not applicable in the context of this assessment, because the safeguard was either explicit and demanding direct (non-technology related) controls; or general, but not allowing for the reasonable use of technology as a compensating control in the fulfillment of the safeguard. Table 2-1 lists the remaining 23 applicable safeguards.

Table 2-1 Applicable Safeguards

	Citation	Title
1.	164.308(a)(1)(i)	Security Management Process
2.	164.308(a)(1)(ii)(D)	Information System Activity Review
3.	164.308(a)(3)(ii)(A)	Authorization and/or Supervision
4.	164.308(a)(3)(ii)(C)	Termination Procedures
5.	164.308(a)(4)(ii)(A)	Isolating Health Care Clearinghouse Function
6.	164.308(a)(4)(ii)(B)	Access Authorization
7.	164.308(a)(4)(ii)(C)	Access Establishment and Modification
8.	164.308(a)(5)(ii)(B)	Protection from Malicious Software
9.	164.308(a)(5)(ii)(C)	Log-in Monitoring
10.	164.308(a)(5)(ii)(D)	Password Management
11.	164.308(a)(6)(ii)	Response and Reporting
12.	164.308(a)(7)(i)	Contingency Plan
13.	164.308(a)(8)	Evaluation
14.	164.310(a)(2)(iii)	Facility Access Control and Validation Procedures
15.	164.312(a)(2)(i)	Unique User Identification

Table 2-1 Applicable Safeguards (continued)

16.	164.312(a)(2)(ii)	Emergency Access Procedure
17.	164.312(a)(2)(iii)	Automatic Logoff
18.	164.312(a)(2)(iv)	Encryption and Decryption
19.	164.312(b)	Audit Controls
20.	164.312(c)(1)	Data Integrity
21.	164.312(d)	Person or Entity Authentication
22.	164.312(e)(2)(i)	Transmission Integrity Controls
23.	164.312(e)(2)(ii)	Transmission Encryption

See Appendix C, "Reference Architecture Assessment Report—Cisco Healthcare Solution," for the complete rationale of how HIPAA controls are divided between technology and policy.

Industry Standards

Although HIPAA is flexible and technology-neutral, industry standards are often used to meet the requirements. Among the standards often used are the NIST Special Publications, ISO 27002 and the HiTrust Common Security Framework (CSF). These standards provide more detail for the design and implementation of the infrastructure to meet the requirements.

The HiTrust alliance was formed by organizations in the healthcare industry to create a detailed framework to meet the vague HIPAA safeguards. Cisco's Solution Framework is closely aligned with the HiTrust CSF and can be used to address many of the detailed security controls in the CSF.

This document addresses HIPAA safeguards directly.

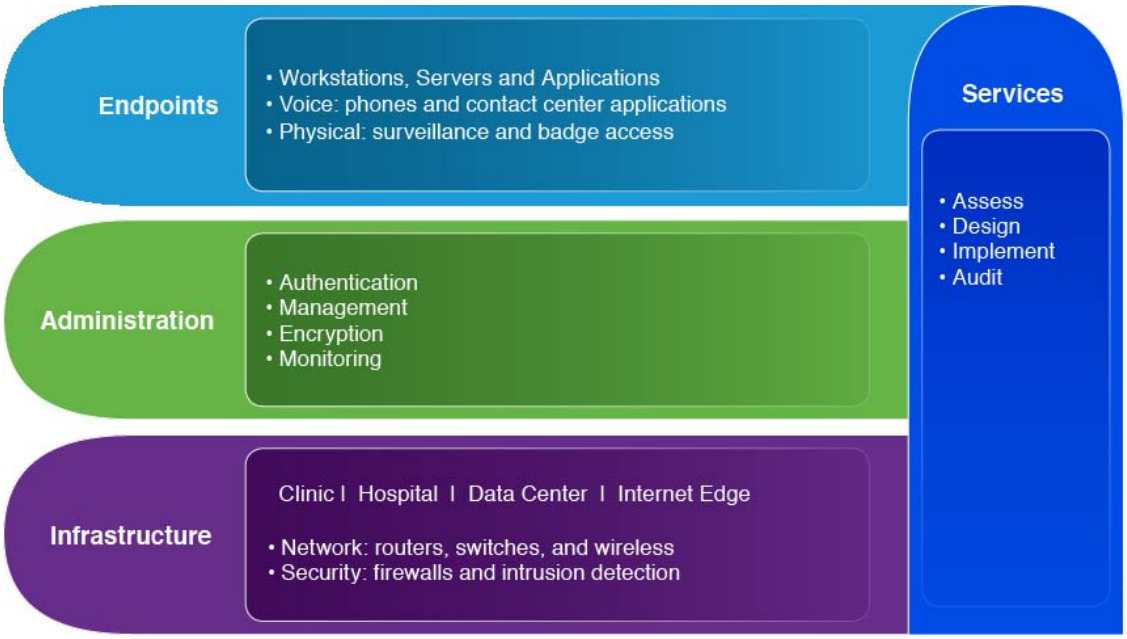
Control Mapping to the Cisco Reference Architecture

Verizon found that Cisco's solution architecture can directly address HIPAA safeguard requirements for technical controls to protect healthcare data. Any device that transmits or stores PHI data needs to be secured. An enterprise network can be conceptualized into several layers, creating a framework that ensures that these devices are properly handled.

HIPAA Solution Framework

Figure 2-1 shows how covered entities and business associates can be organized into a solution framework. By using this framework, healthcare security requirements and their associated control options can be simplified into three overarching layers that allow a simple way of discussing the complexity of the topic. The rest of this manual presents healthcare solution components within this context.

Figure 2-1 Cisco HIPAA Solution Framework



The HIPAA solution framework is used throughout this guide as a model for simplification.

Endpoints/Applications

The top layer of the solution framework takes into account applications or endpoints (workstations, clinical systems, medical devices, mobile carts, and doctors' laptops/tablets/phones) that are involved in the presentation of ePHI for use by/with clinicians, patients, and other member of the workforce. This layer includes the individual applications that may store and process ePHI, including:

- Clinical management and electronic records management systems
- Billing and payment systems
- Image management subsystems
- Voice transcription subsystems
- Video conferencing subsystems

This layer also includes the individual applications that may otherwise provide technical controls that fulfill some element of the HIPAA Security Rule safeguards, including:

- Physical security subsystems
- Emergency voice and data systems
- Data backup subsystems
- Facilities management subsystems

Administration

The middle layer of the framework shows the services used to support administration of the other layers. Example controls include:

- Identity management, authorization, authentication, and access management controls
- Logging and log management controls
- Auditing capabilities
- Monitoring and event management controls
- Data encryption/decryption controls and key management controls
- Physical access, intrusion detection, and surveillance controls

HIPAA is highly focused on Administrative safeguards. 29 of the 52 HIPAA safeguards (9 standards and 20 implementation specifications) are Administrative. To create an environment that is aligned with HIPAA safeguards requires the capability to meet these safeguards. Cisco addresses 13 of the administrative controls.

Infrastructure

The bottom layer of the framework addresses infrastructure components such as routers, switches, firewalls, and security components that support the common and advanced security controls managed at the layers above. The HIPAA Solution framework leverages the inherent strengths of the Cisco network and systems building blocks to allow the customer to build and configure robust architectures that support and align with the HIPAA Security Rule safeguards. The Cisco solution is a set of architectures, strategic principles, and tactical designs meant to provide the reader with a clarifying understanding of how the safeguards (and associated security control implementation requirements) are identified in the HIPAA Security Rule, and how real-world implementations of today's best-practice architecture can be efficiently deployed.

Services

The right-hand element that spans Endpoint, Administration, and Infrastructure layers includes services to plan, build, and manage the network to address the HIPAA Security Rule. These can be provided by Cisco, Cisco partners, and Verizon Business. Sample services can include the following:

- Strategy and analysis
- Assessments
- Design
- Validation
- Deployment
- Migration
- Product and solution support
- Optimization and operation services

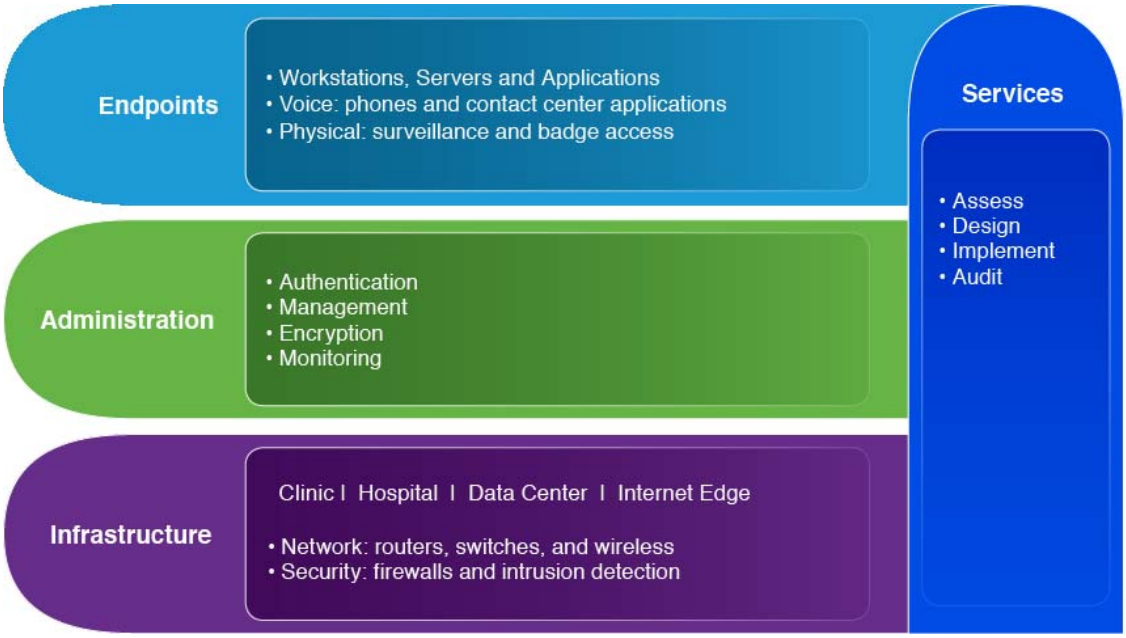
CHAPTER 3

Solution Architecture

Cisco's Compliance Solution for HIPAA Security Rule is a set of architectures, strategic principles, and tactical designs that provide a clarifying understanding of how the network can be used to address HIPAA requirements. Cisco's solution architecture is used as a baseline for demonstrating the range of places that typically exist within an enterprise healthcare provider. This chapter describes the solution architecture in detail so that the HIPAA Security Rule controls can be placed in context. The solution looks at an enterprise from an end-to-end perspective; from a clinic or hospital, where doctors use protected health information (PHI), to the back-end of the data center, where the PHI leaves the providers network to be handled by a business associate.

The Infrastructure layer of the framework shows enterprise locations such as the clinic, hospital, data center, and the Internet edge. The following sections in this chapter show the architectural design considerations of each of these locations. (See Figure 3-1.)

Figure 3-1 Solution Framework



Enterprise Architecture and HIPAA Design Considerations

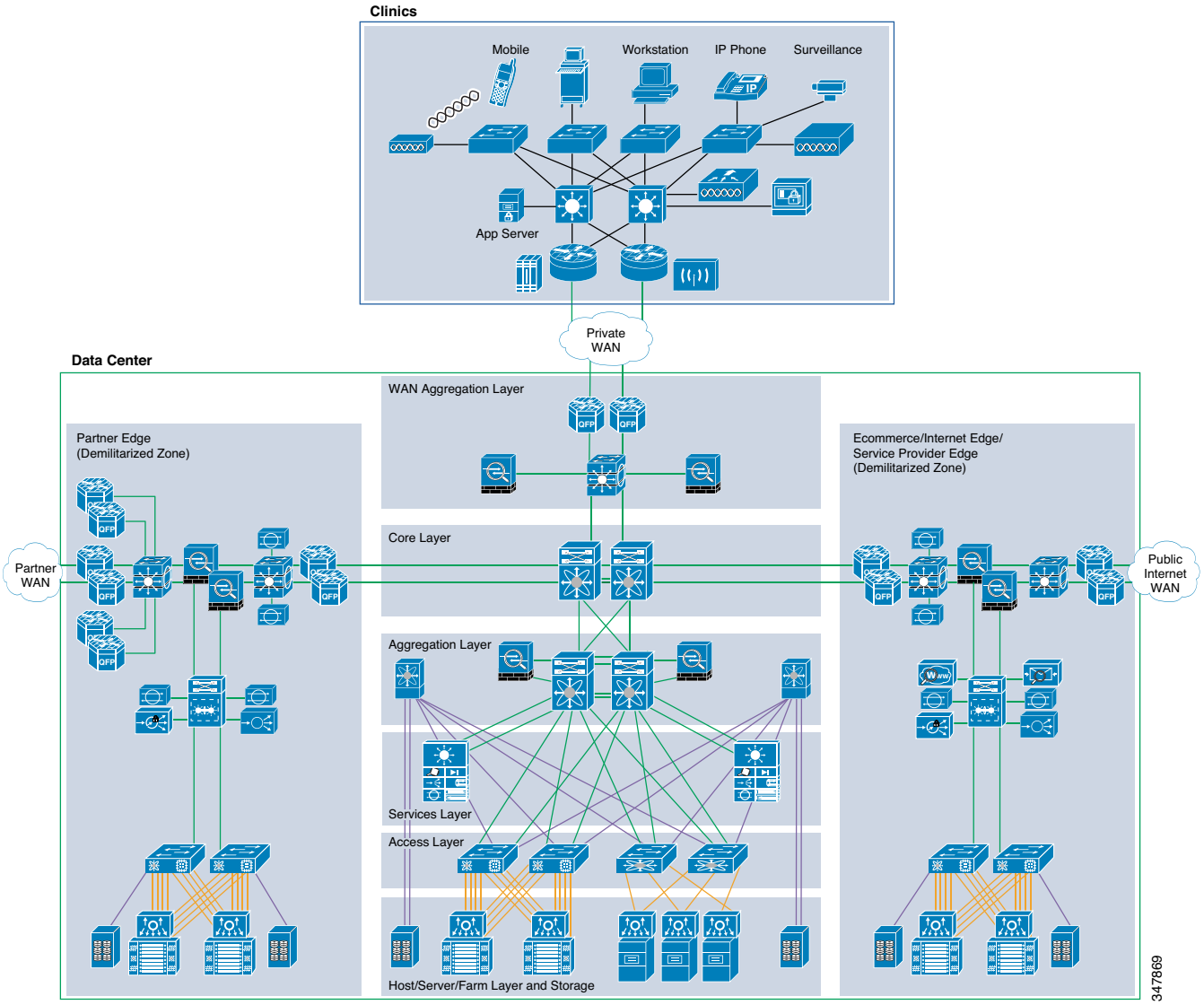
Enterprise Architecture and HIPAA Design Considerations

Healthcare Security control requirements that are derived from the HIPAA Security Rule safeguards apply universally to all sizes of healthcare organization, payer or provider (for example, covered entity), healthcare information clearing houses, Healthcare plans, and Business Associates. The implementation of a secure architecture scales from a single remote clinic to the largest healthcare corporation, with headquarters, regional administrative offices, multiple data centers, points of presence on the Internet, dozens of hospitals, and hundreds of clinics. Cisco's Compliance Solution for HIPAA Security Rule scales both vertically and horizontally to provide the building blocks to construct a compliant enterprise architecture.

Cisco's solution does not guarantee compliance with HIPAA, the ownership of compliance always resides with the covered entity or business associate.

Figure 3-2 shows the enterprise-wide reference architecture and locations that commonly exist in enterprise domain.

Figure 3-2 Enterprise-wide Reference Architecture



Without this contextual reference, it is difficult to discuss specific controls. The following solution principles applied to this architecture reduce risk of losing control of PHI.

- Segmentation

  Within covered entities, the need to segment, separate, and isolate administrative and clinical functions and data is paramount to limiting the scope and depth of security controls that are applied to various forms of data. Generally, institutions that can effectively isolate PHI from other data are most effective at maintaining control over this information. By segmenting clinical information from administrative information, you are able to apply the appropriate controls to effectively protect the information based on its criticality. Enterprise addressing plans should take this into account by separating PHI onto its own address space. Whether in the data center, hospital, or clinic, segregating data leverages the power of the network to help support HIPAA Security Rule safeguards, and best manage risks to PHI and critical medical systems.

  There is an additional benefit beyond security that is a result of effective segmentation. Improved performance can be achieved by designing the architecture to restrict traffic within segments. With the large capacity files for imaging and streaming, this can have a large impact on the response time for healthcare professionals.

- Identity and Access Management

  Identity management, authentication, authorization, and access controls of users/systems to PHI is the central theme in the HIPAA Security Rule safeguards. A strong and manageable identity and access control solution is critical for warranting an assessment of low risk under a customer's risk management program. Effective identity and access management is critical to an organization's ability to meet the Accounting rule.

- Logging, Auditing, and Monitoring

  The need to log, audit, and monitor the access to PHI by users and systems is a critical requirement in the HIPAA Security rule. Centralized application/database/device access logging as well as support for auditing is critical to effectively supporting a covered entity or business associate's breach management strategy. Real-time intrusion detection and protective response within very large and complex networks is critical to identifying compliance issues before they turn into breaches. Logging, auditing, and monitoring are critical to an organization's ability to meet Accounting Rule 164.528, and can help identify whether a compromise has occurred that may lead to a breach notification.

- Encryption

  The ability to encrypt and decrypt PHI represents the most effective and organic control available to resist unwanted PHI data exposures. This applies to HIPAA Safeguard 164.312(a)(1)(2)(iv) Encryption and Decryption.

The following sections describe the major places affected by HIPAA compliance throughout the enterprise. Each section provides design considerations that are affected by HIPAA controls in more detail.

Hospital and Clinic Architectures

Hospitals and clinics provide in-patient and out-patient medical treatment and emergency medical treatment. Each involves creating, receiving transmitting, and maintaining PHI in the forms of electronic medical records, as well as patient treatment information in multiple formats (video, audio, converted photographic and x-ray images, and electronic imaging, and so on).

Design Considerations

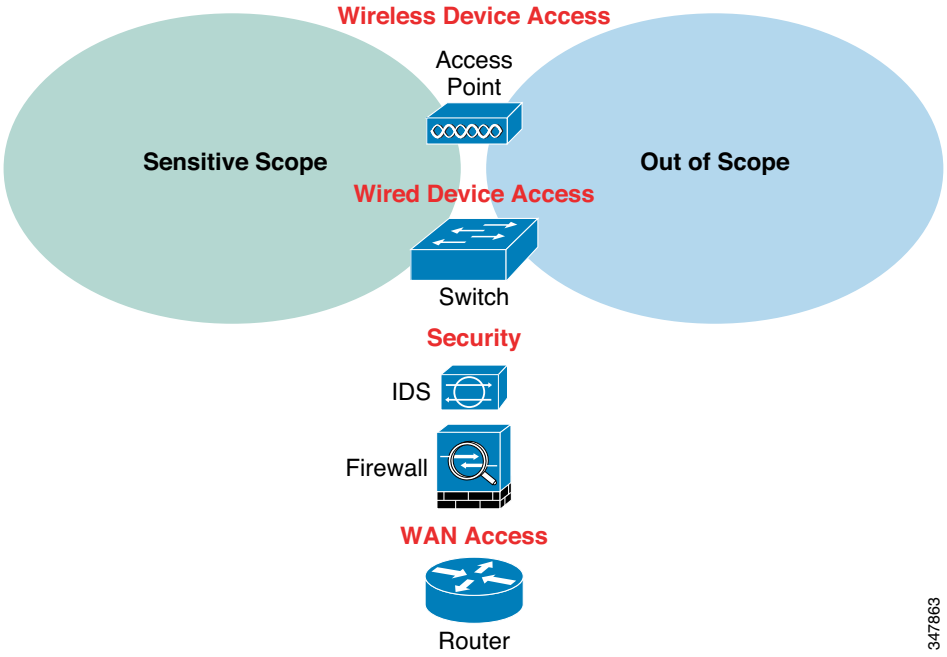
The process of segmenting the wired or wireless networks into *scopes* (that is, devices containing PHI from other devices) is fundamental to demonstrating control and knowledge of the location and use of PHI, as required under HIPAA's Risk Management requirement. The scope of the risk management program and cost of additive control for HIPAA is limited by controlling scope.

Clinics that do not collaborate or share patient data should be isolated from other clinics that do limit the unintentional flow of PHI between them. Consider the isolation of operating units from one another, and from non-required systems in the data center, and the grouping of like functions across segments (for example, LAN/WAN, Internet).

In addition to segmenting, separating, and isolating PHI from other data, VLAN capabilities establish device common "virtual rails" for medical devices, workstations, servers, mobile devices, physical security devices using IP transport, and so on, to simplify control policies between device types and devices.

Figure 3-3 shows the fundamental infrastructure components used within a healthcare location. These components are used in conjunction with each other to segment PHI data from other data.

Figure 3-3 Fundamental Infrastructure Components



Hospital or clinic component designs may scale or consolidate because of the relative size and complexity of the facility, but security functionality is maintained, and each device in the infrastructure is used for a different function.

- The router function can be used for the following:
  - Accessing the WAN
  - Routing between VLANs
  - Providing basic isolation via access control lists (ACLs)

    Routing and access control lists provide segmentation between authorized and unauthorized access on the network. This applies to the HIPAA requirement for preventing, detecting, and containing security violations as listed in the Security Management Process 164.308(a)(i); and protecting ePHI from parts of an organization that are not authorized such as Isolating Healthcare Clearinghouse Functions 164.308(a)(4)(i). Segmentation also provides for protection against malicious software 164.308(a)(5)(ii)(B) and can modify the accessibility as described in Access Establishment and Modification 164.308(a)(4)(ii)(C).
- The firewall can be used for the following:
  - Filtering inappropriate network packets (data, service requests, service acknowledgements, and so on) via a stateful firewall and supporting security policy controls at the boundary edge; for example, limiting inappropriate clinic-to-clinic cross traffic.
  - Routing between VLANs

    The firewall filtering and routing provide segmentation between authorized and unauthorized access on the network. This applies to the HIPAA requirement for preventing, detecting, and containing security violations as listed in the Security Management Process 164.308(a)(i); and protecting ePHI from parts of an organization that are not authorized such as Isolating Healthcare Clearinghouse Functions 164.308(a)(4)(i). Segmentation also provides for protection against malicious software 164.308(a)(5)(ii)(B).
  - Detecting and preventing intrusions; (IPS/IDS devices can also be separate appliances) based on the same security policy; for example, detecting and preventing access attempts from non-clinic personnel.

    The IPS/IDS identifies and notifies appropriate individuals that suspicious activity is occurring. This applies to the HIPAA requirement for identifying and responding to suspected or known security incidents (164.308(a)(6)(ii)).
- Intrusion Prevention Systems (IPS)/Intrusion Detection Systems (IDS) monitor for anomalous behavior on the network and alerts administrators (for example, of issues or attacks that are across multiple servers in a hospital or multiple clinics).
  - The IPS/IDS identifies and notifies appropriate individuals that suspicious activity is occurring. This applies to the HIPAA requirement for identifying and responding to suspected or known security incidents (164.308(a)(6)(ii)).
- The switch can be used for the following:
  - Segmenting via VLANs

    This applies to the HIPAA Safeguard for guarding against malicious software as described in 164.308(a)(5)(ii)(B).
  - Accessing wired devices
- The access point can be used for the following:
  - Filtering between authorized and unauthorized access on the network. This applies to the HIPAA requirement for preventing, detecting and containing security violations as listed in the Security Management Process 164.308(a)(i).
  - Supporting wireless segmentation to match the security policy being asserted in the wired network. Segmentation also provides for protection against malicious software 164.308(a)(5)(ii)(B).

– Accessing wireless devices

The function of each of these devices can be virtualized and consolidated for simplicity, depending on the space and management requirements of the facility footprint. For example, many clinics that occupy leased space are not in control of their IT closet, and may have several power, wiring closet, rack, and cabling restraints that benefit from virtualized devices that reduce the physical footprint of the infrastructure.

Identity and Access Management should be centralized, as is discussed in the data center section. However, when connectivity is lost to the centralized services, local identity and access management should be configured for emergency access.

Logging should be centralized and is discussed in the data center section. However, local device logging should be enabled if centralized connectivity fails. This ensures that auditing and monitoring can be used.

Encryption of PHI across networks is necessary as described in the HIPAA Security Series published by HHS: Covered entities must consider the use of encryption for transmitting ePHI, particularly over the Internet. As business practices and technology change, situations may arise where ePHI being transmitted from a covered entity would be at significant risk of being accessed by unauthorized entities. Where risk analysis shows such risk to be significant, a covered entity must encrypt those transmissions under the addressable implementation specification for encryption; there should be application layer encryption, but additional consideration should be given when PHI leaves the clinic over Internet service provider (VPN) or wireless networks (WPA2).

Conversely, in clinics that own their own space, are moderate size, or have a number of clinical subsystems and technology tools, each of these devices can be increased in number depending on the resiliency and redundancy requirements of the business. For example, if clinic connectivity is a business priority, using redundant routers for redundant WAN access might be a requirement to ensure that connectivity is maintained.

Clinics routinely have minimal space for the technology infrastructure. The ability to implement the technological components securely in minimal space is an advantage.

Regardless of how the IT infrastructure is designed from an ownership and scale perspective, the same types/locations of controls should be consistent and available across the various configurations.

From a control prospective, most health groups “home run” their Internet access from the remote clinics and connected hospitals into their central data center to more effectively manage Internet access, filter content, and enforce data loss prevention, control email connectivity and provide for email filtering in both directions.

This perimeter is typically secured as a demilitarized zone (DMZ) using firewalls and IDS/IPS. Whenever you introduce any type of untrusted network (wireless, Internet, microwave, satellite, cellular, and so on) into the healthcare environment, you have effectively created a new external perimeter that must now be secured with a firewall and intrusion detection/prevention system. Table 3-1 defines the types of factors that affect clinic controls and requirements.

Table 3-1 Healthcare Services and Corresponding Compliance Controls Located at Facility

Hospital/Clinic Service Types	Controls Recommended	Relevant Solution Products
Electronic medical records (EMR) systems	Data encryption/decryption Auto-log-off controls Passwords	Cisco Identity Services Engine (ISE), wireless IPS, 802.1x Switch
Wired and wireless medical devices	Data encryption/decryption Auto-log-off controls Passwords	Cisco Identity Services Engine (ISE), wireless IPS, 802.1x Switch

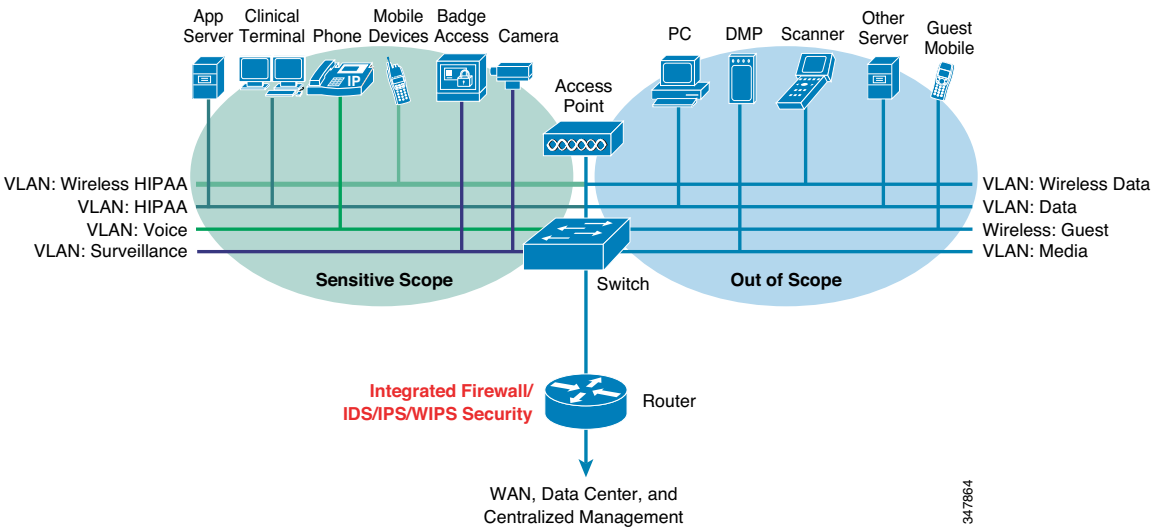
Table 3-1 Healthcare Services and Corresponding Compliance Controls Located at Facility

Imaging systems	Data encryption/decryption Auto-log-off controls Passwords	Cisco Identity Services Engine (ISE), wireless IPS, 802.1x Switch
Wireless tablets and roll-around carts	Data encryption/decryption Auto-log-off controls Passwords	Cisco ISR, Cisco ASA, Cisco IPS appliance, Cisco Unified Wireless
Hospital/clinic LAN/WAN	Firewall, IDS	Cisco Integrated Services Router (ISR), Cisco Adaptive Security Appliance (ASA), Cisco IPS Appliance
Patient registration workstations Nurse station workstations	Authentication controls Passwords	Cisco Identity Services Engine (ISE), wireless IPS, 802.1x Switch
Internet demarcation	Data encryption/decryption Firewall, IDS	Cisco Integrated Services Router (ISR), Cisco Adaptive Security Appliance (ASA), Cisco IPS Appliance

The fundamental reference architecture assumes that a covered entity or business associate may eventually need to scale to these levels of services, but not necessarily immediately. From a facility perspective, Cisco's Integrated Services Router (ISR) performs each of the functions listed in Table 3-1. This allows a provider to grow with its investment by purchasing a router that can scale by different license keys for different services without having to rip and replace. For example, a clinic can purchase an ISR for basic WAN connectivity. When the business wants to introduce wireless to the facility, the merchant can unlock the firewall/IPS/IDS feature set with a license.

The fundamental healthcare reference architecture in Figure 3-4 shows the solution framework endpoints/applications within the context of the fundamental healthcare component's infrastructure.

Figure 3-4 Fundamental Reference Healthcare Architecture



In-scope devices can include the following:

- Medical devices and imaging subsystems
- Mobile video/audio carts and wireless tablets
- Physical access, ID, and surveillance subsystems for the facilities
- Clinical and administrative workstations
- Primary EMR servers

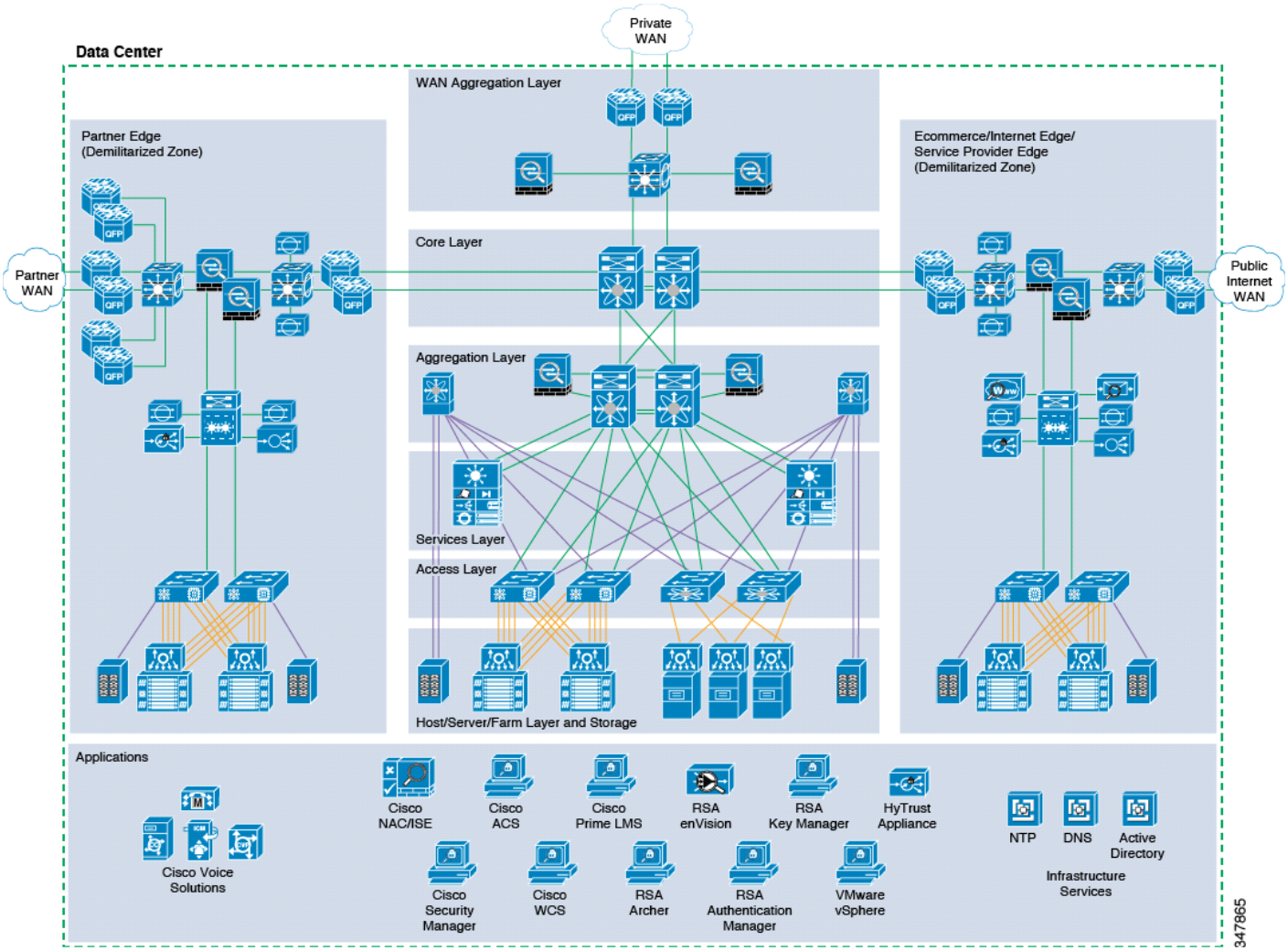
In general, an additional VLAN for management of infrastructure should be distinctly defined. The remaining devices at the facility level are considered *out-of-scope* and do not need to be audited, given that they are on their own network and segmented via firewall/IPS/IDS from the sensitive networks.

The HIPAA facility model and its controls were applied to multiple healthcare formats ranging from clinics to hospitals and are shown in Chapter 4, "Solution Implementation," in detail. This section provides sample addressing plans used. Many designs can be extracted by understanding and using the Healthcare Reference Architecture shown above, but the overall functions are essentially the same.

Data Center

The data center provides a covered entity or business associate with the ability to centralize, aggregate, consolidate, share, maintain, and control their storage of PHI. (See Figure 3-5). The data center is also the place where management systems are deployed. The data center provides centralized control from an administrative perspective because administrative and management tools can span across the data center servers, hospital systems, and remote clinic systems. This minimizes operational overhead and enforces the security policy.

Figure 3-5 Data Center Architecture



Design Considerations

Data centers can house many types of functions and the term itself can encompass narrow and broad aspects. For the purposes of this guide, data centers include the following functions:

- WAN aggregation layer—Aggregates the clinic and hospital WAN connections to the core
- Core layer—Highly available, high-speed area that is the central point of connectivity to all data center areas
- Aggregation layer—Aggregates the services of one area and connects that area to the core
- Services layer—Data treatment and manipulation occurs between access layer and aggregation layer
- Access layer—Server-level access and connectivity between hosts/servers to the services and aggregation layers, depending on the nature of the application
- Host/server farm—Physical servers, virtualized servers, and appliances' host applications
- Storage—Storage area networks (SANs)
- E-commerce/Health—Internet-based transactions for prescription renewals, payment of bills
- Internet/service provider edge demilitarized zone (DMZ)—Secure connectivity to the Internet
- Partner edge DMZ—Secure segmented connectivity to partners

Common data center security features include, but are not limited to, the following:

- Standardized equipment and software images that are deployed in a modular, layered approach simplify configuration management and increase the systems availability.
- The highly available data center design permits highly resilient access from clinics to core data and storage services.
- WAN aggregation alternatives allow flexible selection of service provider network offerings.
- The service aggregation design allows for a modular approach to adding new access layers and managing shared network services (for example, firewall, IDS, application networking, wireless management)
- Firewall, IDS, and application networking services are available at the service and aggregation layers of the data center.
- Scalability accommodates shifting requirements in data center compute and storage requirements.
- WAN access speeds are typically the limiting factor between the clinic network systems and the WAN aggregation layer.
- Backup network connections from remote facility networks to the data center are recommended when PHI is transported via the WAN.

Related to segmentation between clinical and other systems, clinical data should be, to the extent possible isolated to reduce the risk of copying PHI on to non-PHI data sets, databases, file, file shares, or system drives and backups. Isolation can be accomplished at both the system and network levels by organizing clinical systems in separate VLANs from other systems, and by enforcing access restrictions between dissimilar system/server functional groups. HIPAA 164.308(a)(4) Isolating Clearinghouse Functions requires that covered entities must create separation of PHI from the larger organization, which can be accomplished through router/switch segmentation functionality or through the use of firewalls to more effectively manage a uniform segmentation "policy" across multiple devices and interfaces. Consideration should be given to isolating PHI traffic between servers to a common and small (for example, controllable) set of VLANs, to the exclusion of other systems.

Related to segmentation between internal data center systems and Internet-exposed components, an organization must have policies and procedures in place for preventing, detecting, and containing security violations as listed in the Security Management Process 164.308(a)(i). Additionally, HIPAA §164.312(c)(1) Data Integrity mandates procedure (or technical controls) to protect PHI from improper alteration or destruction. The use of firewalls as a demarcation and access management point allows the customer to establish and manage a common security policy for data flows between data center and Internet-exposed devices/systems to support maintaining data integrity around PHI. Along with strong application and system controls, the use of network restrictions aligns with the defense-in-depth strategy. Obfuscate internal addressing schemes to the public, especially addresses of PHI storage devices and backups. Consider the use of enterprise-class firewalls to provide a unified security policy management framework to manage critical network boundaries between the covered entity/business associate and the rest of the Internet.

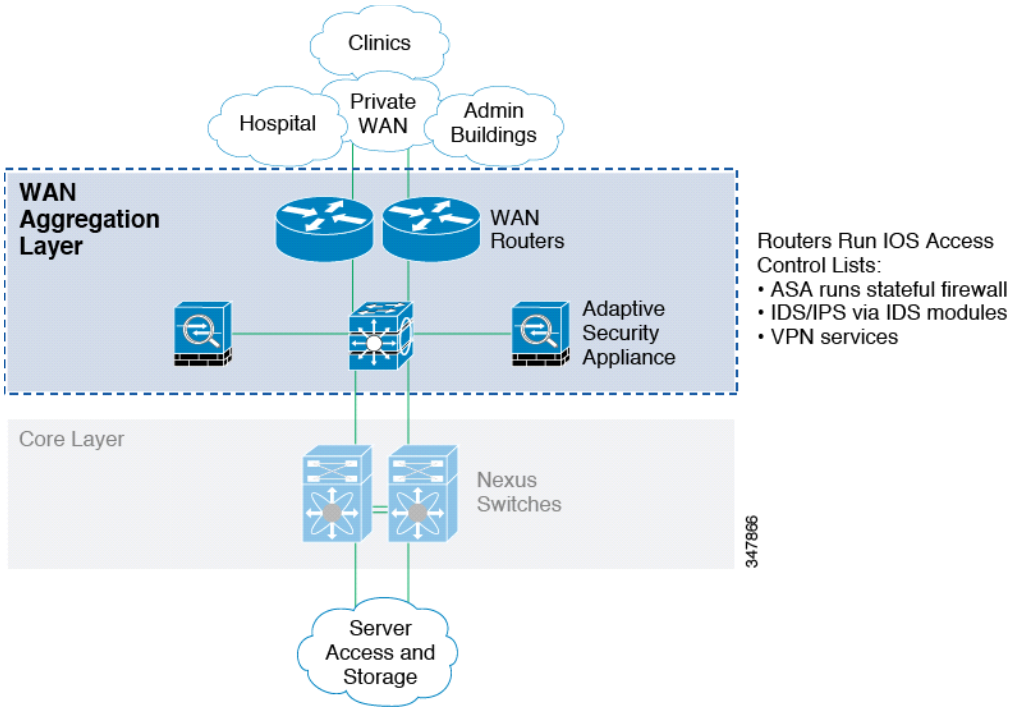
Identity management, authentication, and authorization of users and systems to PHI; and access controls between users/systems and PHI is critical to enforcing HIPAA safeguards. Having the ability to individually grant or deny access to a user or by system at the network (device) and/or system (server) levels provides the granularity of control necessary to support HIPAA safeguards. Consider leveraging centralized identity and access management functions across health groups, and within hospitals and clinics to best support restriction of users and systems to PHI. Ensure that the ability to control access during both routine and emergency access is supported. 164.312.(a)(1) Access Control requires that technical policies and procedures be implemented to allow access only to persons or software programs that are authorized.

An ability to seamlessly encrypt and decrypt PHI and to share encrypted files across the network provides opportunities for real-time PHI sharing and collaboration to improve patient care. The ability to seamlessly exchange PHI or various types, all in encrypted form, reduces the potential places where PHI can be breached. Encrypt PHI (and all operating data if possible) while in transit across the enterprise and when transiting the Internet or other public networks. Consider leveraging encryption management and engines to encrypt/decrypt all PHI when stored. Providing the capability to encrypt traffic sent over public networks helps an organization meet the HIPAA requirement for Transmission Security 164.312(e)(1), Integrity 164.312(e)(2)(i), and Encryption 164.312(e)(2)(ii).

WAN Aggregation

The WAN aggregation layer is a transit network that aggregates the connections from the healthcare locations, backstage locations, and offices, as shown in Figure 3-6.

Figure 3-6 WAN Aggregation Layer



Design Considerations

Segmentation is used at the WAN aggregation layer to minimize the PHI scope from sites that do not have PHI. The WAN aggregation layer needs Layer 3 filters to restrict PHI data from crossing into sites that do not have the need for PHI data.

Two options are possible at this layer for Layer 3 filters at the WAN aggregation layer:

- Firewall appliance—Interior to the WAN edge routers, a dedicated firewall appliance is used to secure incoming WAN traffic and to terminate remote facility VPN connections. This design provides the highest scalability. When managed centrally over several firewalls, a unified security policy can be exerted over the organization with the minimum of administrative overhead, and in a repeatable way that supports effective risk management. The firewall provides multiple safeguards to help a healthcare organization meet HIPAA safeguards. The firewall filtering and routing provide security between authorized and unauthorized traffic from an unsecured network. This is extremely important when connecting the organization to external networks such as the Internet or a business associate. This helps an organization meet the HIPAA requirement for preventing, detecting, and containing security violations as listed in the Security Management Process 164.308(a)(i).

- Cisco IOS Software firewall routers—Many Cisco routers also support the Cisco IOS security software option that includes a firewall feature. Cisco recommends the use of the Cisco IOS Security feature set in hospitals, branches, and teleworker deployments, because of a much lower number of users and connection rates than at the Clinic WAN aggregation head end location.

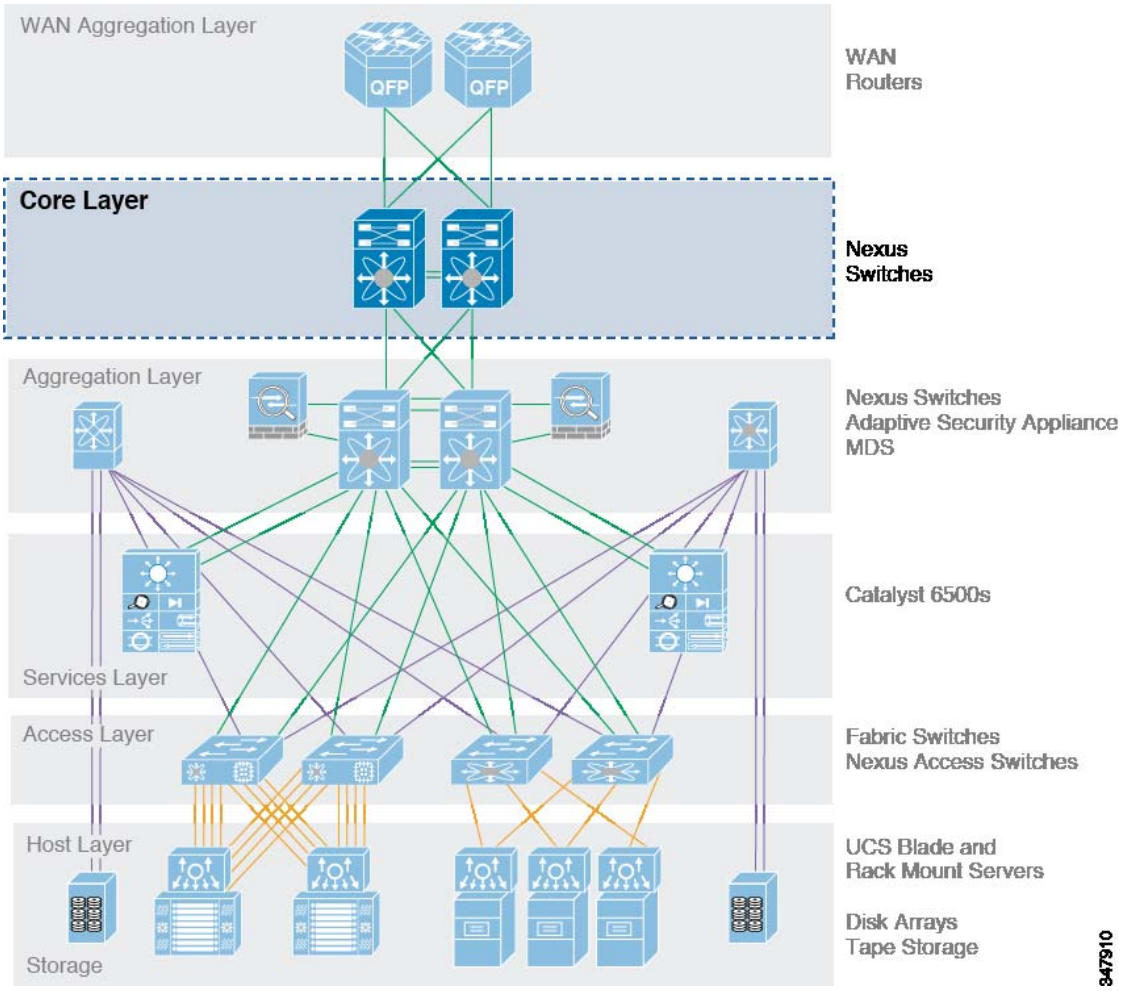
There are two typical WAN speed categories for a WAN aggregation network: less than and up to OC3 (155 Mbps), and OC12 (622 Mbps) and above. The choice of these two network speeds determines the platform set to select from Cisco. In addition, this design creates two profiles for each WAN speed. These profiles are designed to provide guidance when designing a WAN edge network, regardless of which enterprise WAN architecture is selected. The profiles for each WAN speed investigate integrated versus dedicated chassis for each functionality component, as highlighted in the previous section. Some customers prefer a highly integrated solution where most, if not all, of the WAN edge functions described in this document reside on a single or very few network devices. Other customers prefer the granularity and scalability of these same functions separated across multiple network devices.

The WAN aggregation architecture is based on the *Infrastructure Protection and Security Service Integration Design for the Next Generation WAN Edge v 2.0*, which can be found at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/IPSNGWAN.html

Core Layer

The core layer provides the high-speed packet switching backplane for all flows going throughout the data center, as shown in Figure 3-7.

Figure 3-7 Core Layer



Design Considerations

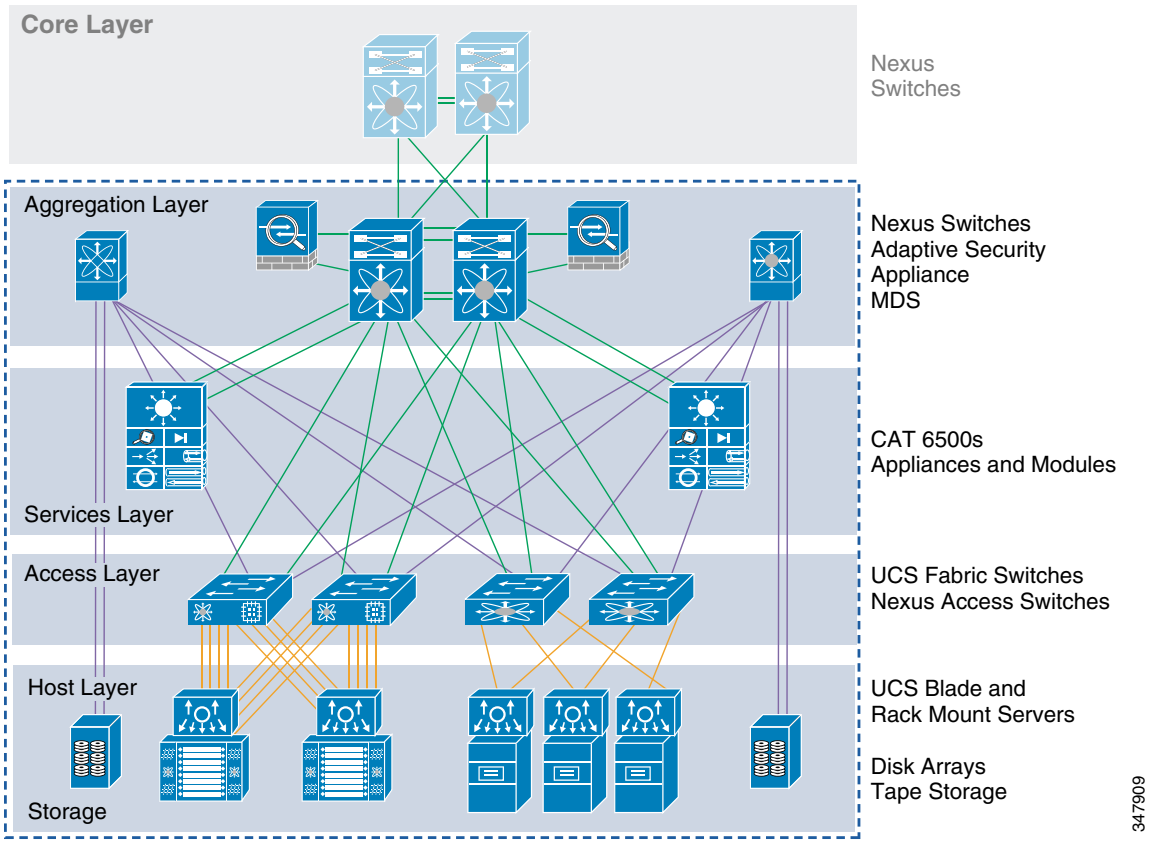
Depending on the risk management strategy, high availability may be a requirement. The core is the fundamental layer of an enterprise architecture that provides high availability and connectivity between all other layers. The core layer provides connectivity to multiple aggregation layers and provides a resilient Layer 3 routed fabric with no single point of failure. The core layer runs an interior routing protocol, such as Open Shortest Path First (OSPF) or Enhanced Interior Gateway Routing Protocol (EIGRP), and load balances traffic between the core and aggregation layers using the Cisco Express Forwarding (CEF)-based hashing algorithms. The core is not a perimeter; no security filtration should be performed at this layer. The core layer support the efficient transport of clinical, imaging, and administrative data without throughout issues or bottlenecks, thereby ensuring the highest patient care through data availability to the care team.

The core, services aggregation, and server access tiers of the multi-tier data center architecture was based on the design documented in the *Cisco Data Center Infrastructure Design Guides*, which can be found at the following URL:
http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns743/ns994/landing_dc_infrastructure.html

Aggregation Block

An aggregation block is a combination of the aggregation, services, and access layer systems. It represents a repeatable, implementable template for scaling applications and services within the data center. (See Figure 3-8.)

Figure 3-8 Aggregation Block



Design Considerations

Segmentation can occur at this layer by separating entire aggregation blocks or within the block. These blocks can be zoned by function or compliance types. For example, an organization that has sensitive healthcare information may be zoned away from the payment card sensitive information. Zones are a best practice to isolate applications and services based on their individual policy requirements. You can

securely mix in-scope and out-of-scope applications and services within a single aggregation block but you may use entire aggregation blocks separately to ease administration as policies change over time. The aggregation layer uses Layer 3 filters to segregate and protect the edge of the scope of compliance.

In the services layer, server load balancing and wide-area application services (WAAS) are used at this layer to optimize applications. Using these devices to support HIPAA-relevant applications brings these devices into scope and susceptible to the same safeguards. For more information on understanding these safeguards and controls, consult [Chapter 5, "Component Assessment."]

In the access layer, switches provide both Layer 2 and Layer 3 topologies to enable segmentation within the aggregation block. The solution management servers connect to the network in this layer. They are centralized, segmented from other business application servers, and protected by firewall services from the service aggregation layer above.

In the storage layer, a combination of disk encryption provided by the Cisco MDS encryption card, fibre-channel zoning, and logical unit (LUN) masking/zoning were used in the storage implementation of this solution. By deploying zoning within a Fibre Channel fabric, device access is limited to devices within the zone. This allows the user to segregate devices based on access to a particular storage device (disk array). This applies to HIPAA Safeguard 164.312(a)(1)(2)(iv) Encryption and Decryption. This is a requirement in a data center environment in which multiple file servers in the data center server farm are connected to the same SAN fabric, and access to PHI data must be restricted to a subset of servers. LUN masking takes zoning beyond the Fibre Channel switchport level by restricting access to specific LUNs on a given disk array. Only specific devices belonging to the LUN zone are able to access those sections of the disk. Applications can be grouped by PHI use/storage, with encryption support on some devices but not necessarily on all arrays. Encryption keys for storage are managed by Cisco Key Manager and RSA Data Protection Manager. This provides a uniform method to control encryption keys across the enterprise. Key management can be structured by organizational unit, so the multiple business units can be supported under the same key management scheme, and the potential to intermix or misroute PHI (when encrypted) can reduce the potential for breach. This measure can mean the difference between losing PHI when other security controls are intentionally compromised, and maintaining control over that data.

In the host layer, server virtualization technology can be used to further establish separation between applications containing PHI and other applications, and to organize process-intensive applications into demand-groups to ensure timely file retrieval and update. Individual blades within a blade server chassis can be used to segment sensitive and non-sensitive applications because they run independent hypervisors. Because hypervisors are considered insecure, when mixing sensitive applications with non-sensitive applications (mixed-mode) across the same hypervisor, the non-sensitive applications are now in scope.

While meeting the central focus of this design guide by recommending an architecture that meets the HIPAA Safeguards, additional QoS parameters can increase performance using the recommended segmentation strategies.

For more information, see the following URL:
http://www.cisco.com/en/US/partner/solutions/ns340/ns414/ns742/ns743/ns1050/landing_vmdc.html

The host layer/server farm is where the centralized applications are deployed for managing and enforcing the segmentation policy, logging, auditing, monitoring, identity authentication and authorization.

Table 3-2 lists descriptions of applications for administrators.

Table 3-2 Centralized Toolkit for Administrators

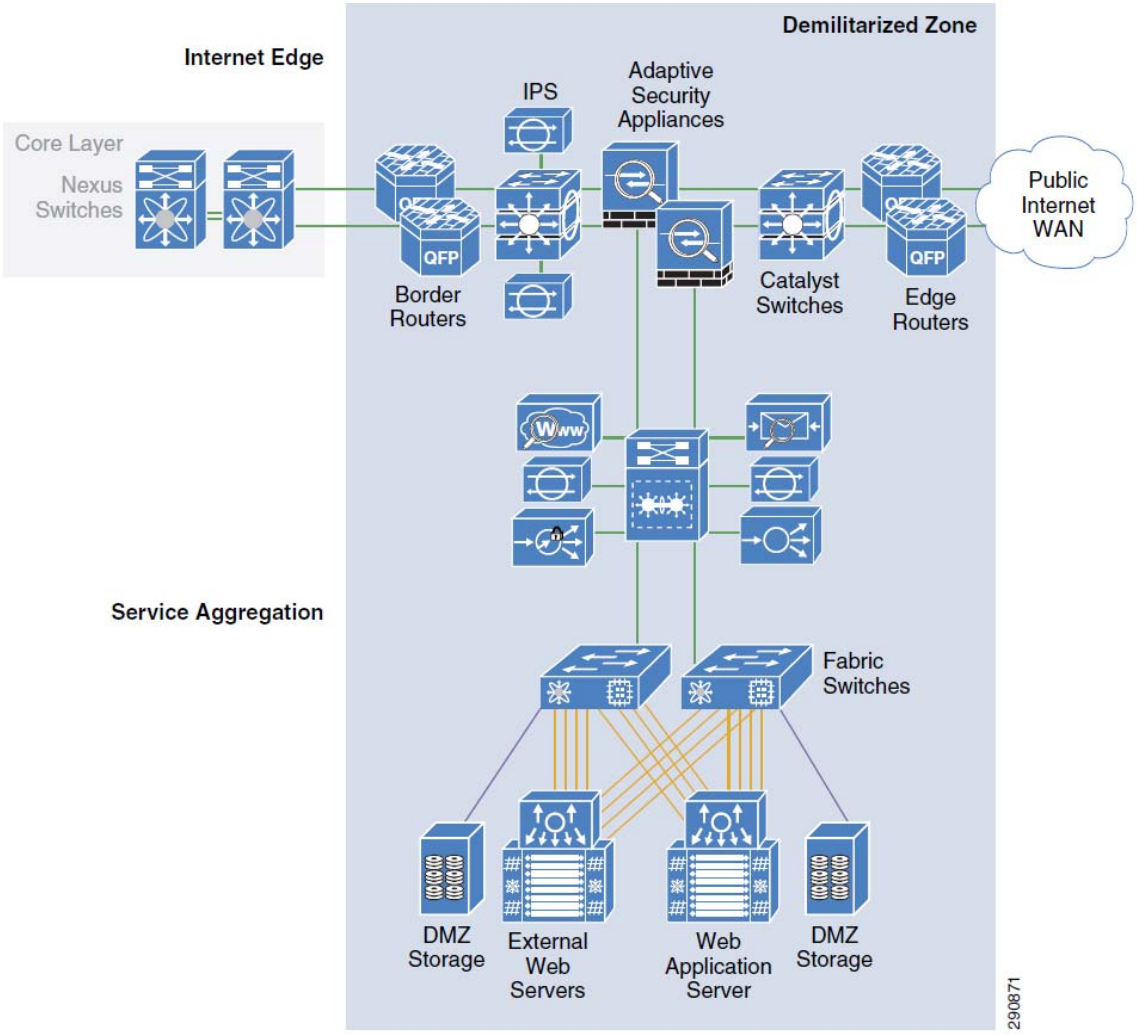
Function	Solution Component Options
Physical Security	
Closet to building access	Cisco Physical Access Manager
IT space intrusion detection	Cisco Physical Access Manager
Video surveillance	Cisco Video Surveillance Manager
Identity Management, Authentication, and Access Controls	
Device AAA	Cisco Secure ACS, Cisco ISE
Two-factor remote	RSA Authentication Manager
Directory services	Microsoft Active Directory
Logging, Auditing and Monitoring	
Event correlation	RSA enVision
Policy enforcement	Cisco Prime LAN Management Solution (LMS)
Corporate policy	RSA Archer
Virtualization	EMC Unified Infrastructure Manager, VMware vSphere
Encryption	
Storage	Cisco Key Manager, RSA Data Protection Manager
Remote access/VPN	Cisco Security Manager, Cisco AnyConnect VPN
Network Management	
Device configuration	Cisco Prime LMS
Security configuration	Cisco Security Manager
Wireless configuration	Cisco WCS

E-commerce/Internet Edge/Service Provider Edge/Partner Edge

E-commerce/Internet Edge/Service Provider Edge/Partner Edge

The solution uses a collapsed Internet edge and extranet network to support Internet connectivity and business partner connectivity, as shown in Figure 3-9.

Figure 3-9 E-commerce/Internet Edge/Service Provider Edge



Design Considerations

The primary segmentation of the perimeter of the enterprise occurs at the edge.

The design does the following:

- Provides an enterprise connection to the Internet.
- Secures the Internet edge design using Cisco firewall and intrusion detection systems.
- Provides a dual-threaded design for network resiliency.

- Provides a collapsed Internet edge and extranet network for a highly centralized and integrated edge network.
- Provides remote VPN access to enterprise users/telecommuters.

This design takes into account best practices from the *Data Center Networking: Internet Edge Design Architecture Design Guide* (http://www.cisco.com/go/designzone) and customizes these recommendations for Internet edge and extranet networks. The edges connect Internet services to the complete enterprise environment from hospitals to Internet service providers and clinic office connections that use a Cisco secure VPN to connect to data centers. The collapsed design provides highly centralized and integrated edge networks, and transports the aggregated traffic through various service modules (Cisco ACE, Cisco ASASM, and Cisco IDSM2) within a pair of Cisco Catalyst 6500 switch chassis. The Internet edge provides the following security functions:

- Secure configurations and management.
- IP anti-spoofing.
- Access control lists (ACLs) provide explicitly permitted and/or denied IP traffic that may traverse between inside, outside, and DMZ. Routing and access control lists provide segmentation between authorized and unauthorized access on the network. This applies to the HIPAA requirement for preventing, detecting, and containing security violations as listed in the Security Management Process 164.308(a)(i); and protecting ePHI from parts of an organization that are not authorized such as Isolating Healthcare Clearinghouse Functions 164.308(a)(4)(i). Segmentation also provides for protection against malicious software 164.308(a)(5)(ii)(B) and can modify the accessibility as described in Access Establishment and Modification 164.308(a)(4)(ii)(C).
- Stateful inspection provides the ability to establish and monitor session states of traffic permitted to flow across the Internet edge, and to deny traffic that fails to match the expected state of existing or allowed sessions. The firewall filtering and routing provide segmentation between authorized and unauthorized access on the network. This applies to the HIPAA requirement for preventing, detecting, and containing security violations as listed in the Security Management Process 164.308(a)(i); and protecting ePHI from parts of an organization that are not authorized such as Isolating Healthcare Clearinghouse functions 164.308(a)(4)(i). Segmentation also provides for protection against malicious software 164.308(a)(5)(ii)(B).
- Intrusion detection using Cisco IDSM2 provides the ability to promiscuously monitor traffic across discrete points within the Internet edge, and to alarm and/or take action after detecting suspect behavior that may threaten the enterprise network. The IPS/IDS identifies and notifies appropriate individuals that suspicious activity is occurring. This applies to the HIPAA requirement for identifying and responding to suspected or known security incidents (164.308(a)(6)(ii)).
- Applications servers that need to be directly accessed from the Internet are placed in a quasi-trusted secure area (DMZ) between the Internet and the internal enterprise network, which allows internal hosts and Internet hosts to communicate with servers in the DMZ.
- All public-facing web applications should be developed using the security best practices to prevent known attacks, and must be reviewed annually or after changes.

The Internet and Partner Edge provides multiple safeguards to help a healthcare organization meet HIPAA safeguards. The firewall filtering and routing provide security between authorized and unauthorized traffic from an unsecured network. This is extremely important when connecting the organization to external networks such as the Internet or a business associate. This helps an organization meet the HIPAA requirement for preventing, detecting. and containing security violations as listed in the Security Management Process 164.308(a)(i).

The firewall also provides encryption capability to encrypt traffic sent over public networks. This helps an organization meet the HIPAA requirement for Transmission Security 164.312(e)(1), Integrity 164.312(e)(2)(i), and Encryption 164.312(e)(2)(ii).

E-commerce/Internet Edge/Service Provider Edge/Partner Edge

The IPS/IDS identifies and notifies appropriate individuals that suspicious activity is occurring. This helps an organization proactively address security incidents. This applies to the HIPAA requirement for identifying and responding to suspected or known security incidents (164.308(a)(6)(ii)).

CHAPTER 4

Solution Implementation

Overview

Cisco customers have asked Cisco to provide insight on how Cisco products can be used to address their HIPAA compliance requirements. To fully accomplish this goal, Cisco hired an auditor and went through the same process as covered entities or business associates. To assess Cisco's products for the capability and applicability to satisfy compliance safeguards and controls, they had to be installed and configured within a representative design.

This chapter demonstrates how the Cisco Compliance Solution for HIPAA Security Rule reference architecture provides a solution that was installed and configured to address commonly understood healthcare security controls. Cisco partnered with RSA, Hytrust, EMC, VCE, and Verizon to create a comprehensive design that reflected the framework and architectural principles discussed in earlier chapters.

Cisco's solution was reviewed and validated in the Cisco lab in San Jose, California. Prototype hospital, clinic, data center, WAN, and Internet edge network infrastructures were built using Cisco's best practice design guides, as represented by the Cisco designs and architectures (http://www.cisco.com/go/designzone). The individual components were installed and configured to best support HIPAA Security Rule control requirements and management of data protection. Verizon conducted an assessment of this design and advised on how Cisco security devices and features could provide direct and compensating controls in support of addressing the administrative, operational, physical, and technical Safeguards called in the HIPAA Security Rule. Verizon Business provided a detailed Healthcare Security Requirements Assessment, provided in Appendix C, "Reference Architecture Assessment Report—Cisco Healthcare Solution."

Tip An ***architecture*** is a strategic structure for the consistent design, construction, and operation of systems to achieve a desired set of outcomes.

A ***design*** is a tactical implementation of an architectural strategy, using specific configurations of products to satisfy business requirements.

Chapter 3, "Solution Architecture," describes the enterprise architecture with regards to compliance. This chapter demonstrates a design or, in other words, a specific implementation of components to achieve these principles. Various designs can result from the solution architecture. The design that was

implemented is not intended to represent the only way that Cisco and partner products can be installed to protect PHI. It is intended to provide an example showing how and what was used to achieve the principles described in Chapter 3, "Solution Architecture."

Although every company has specific considerations that vary from this implementation, these designs and the configurations of the components in Appendix E, "Detailed Full Running Configurations," provide an instructive example of what is needed to secure PHI. Each component selected was assessed for its capabilities and applicability, and that assessment is covered in the next chapter.

In each section, a reference architecture is shown with the corresponding design that was implemented and validated within Cisco's laboratories. The full configurations of each individual component are available in Appendix E, "Detailed Full Running Configurations."

Infrastructure

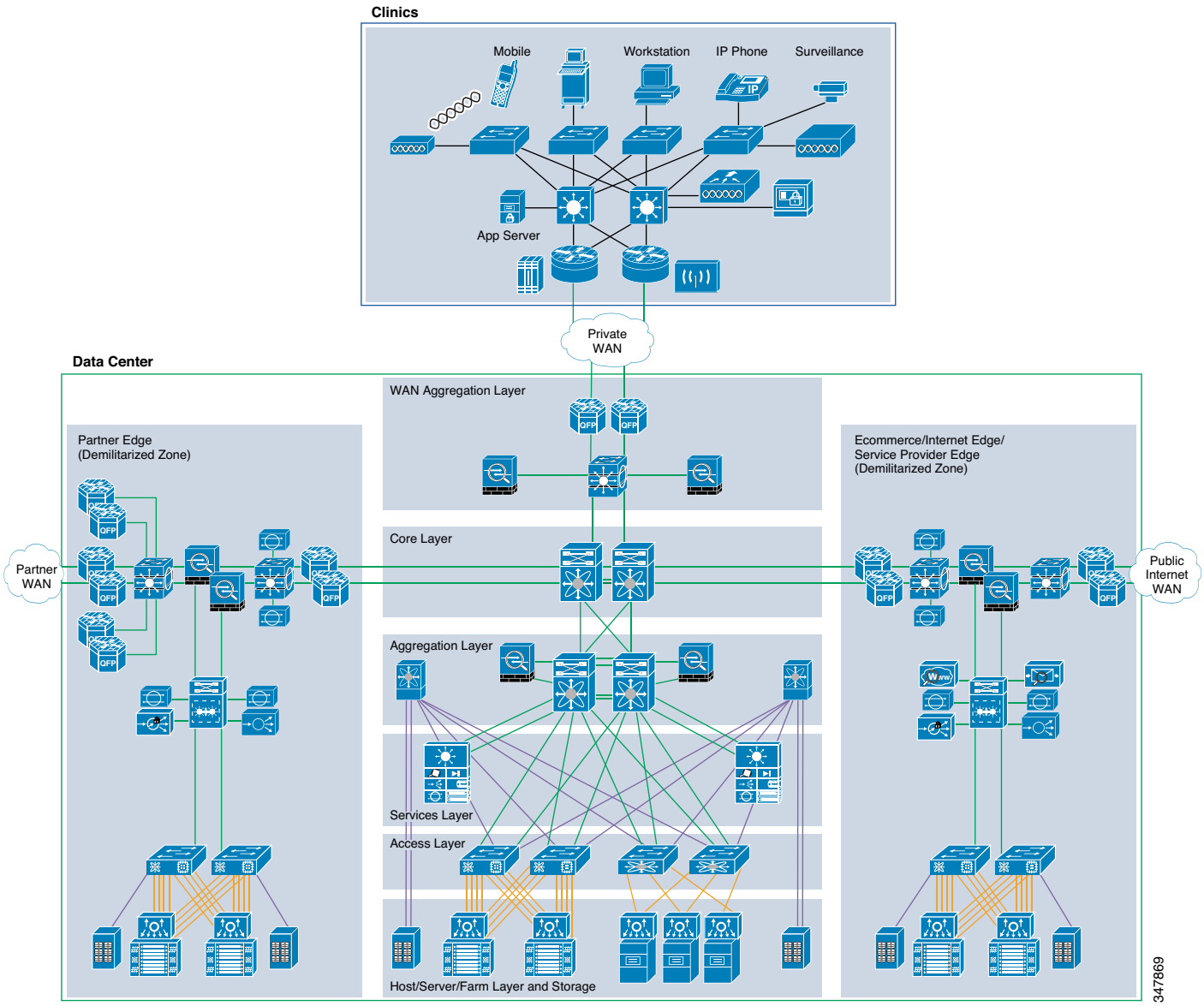
The infrastructure layer of the solution framework addresses the components such as routers, switches, firewalls, and security components. These are used for reference architectures for a variety of locations such as hospitals or data centers as shown in Figure 4-1.

Figure 4-1 Infrastructure Layer of the Solution Framework

The following sections describe the designs that were implemented from the reference architecture.

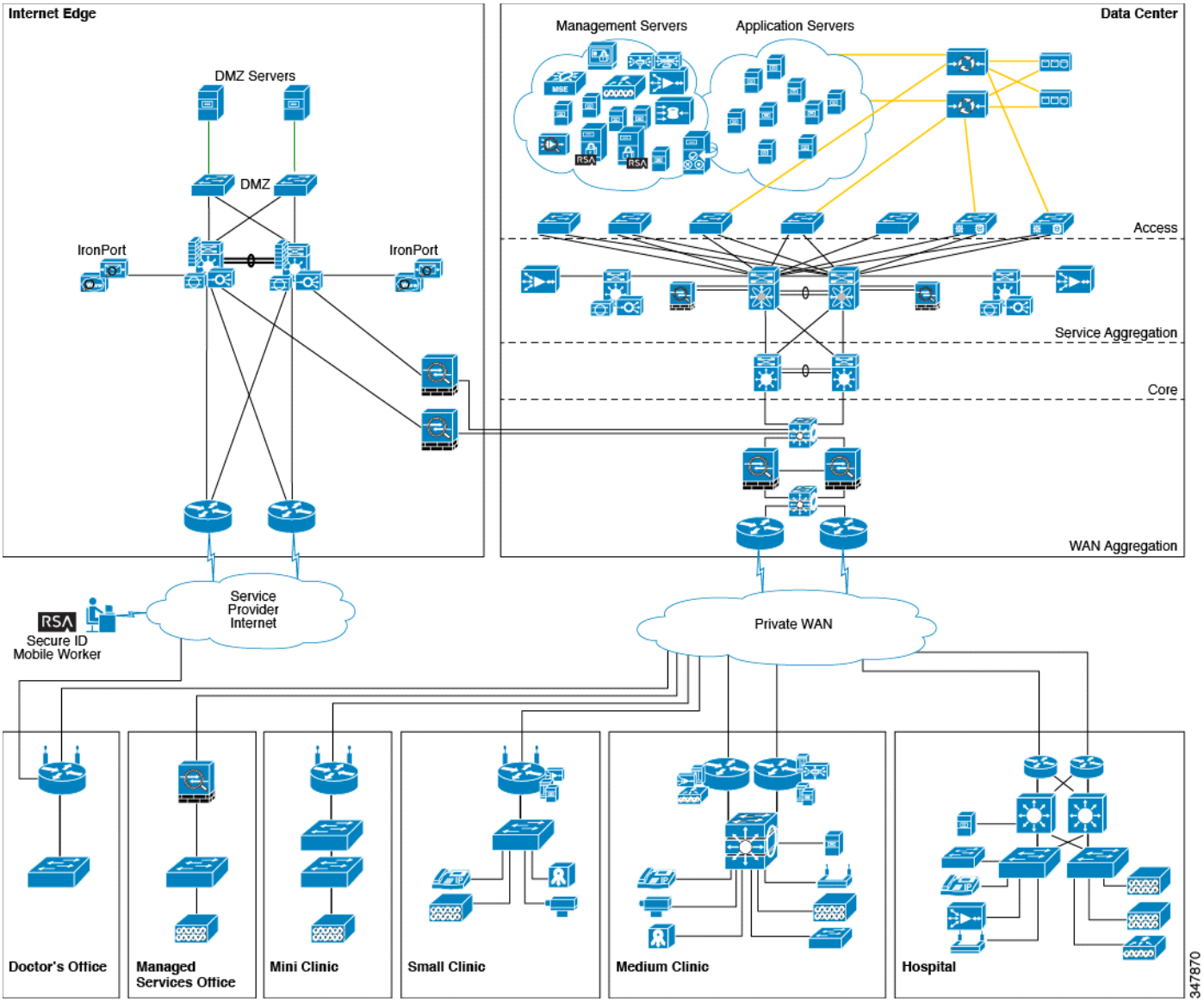
Figure 4-2 shows the enterprise-wide reference architecture.

Figure 4-2 Enterprise-Wide Reference Architecture



Referencing an enterprise-wide architecture as shown in Figure 4-2, the design shown in Figure 4-3 was created in the Cisco lab.

Figure 4-3 Cisco Lab Reference Architecture



Note the following:

- Three clinic designs and one hospital design were elected to represent typical healthcare group IT needs.
- The data center consists of a single aggregation block based on the Data Center 3.0 architecture.
- The Internet edge is representative of both the e-commerce/health and partner edge for the purposes of validation.

The following sections describe this enterprise-wide design in more detail, and demonstrate what was implemented within the lab.

Healthcare Facilities—Clinics and Hospitals

Multiple healthcare facility footprints were implemented that address a variety of business objectives. Each footprint section contains designs that were extracted from the reference architecture. Each design contains the following:

- Reference architecture
- Healthcare facility design
  - Logical topology
  - Addressing plan
  - Components selected

For component compliance functionality, see Chapter 5, "Component Assessment." For full device configurations, see Appendix E, "Detailed Full Running Configurations."

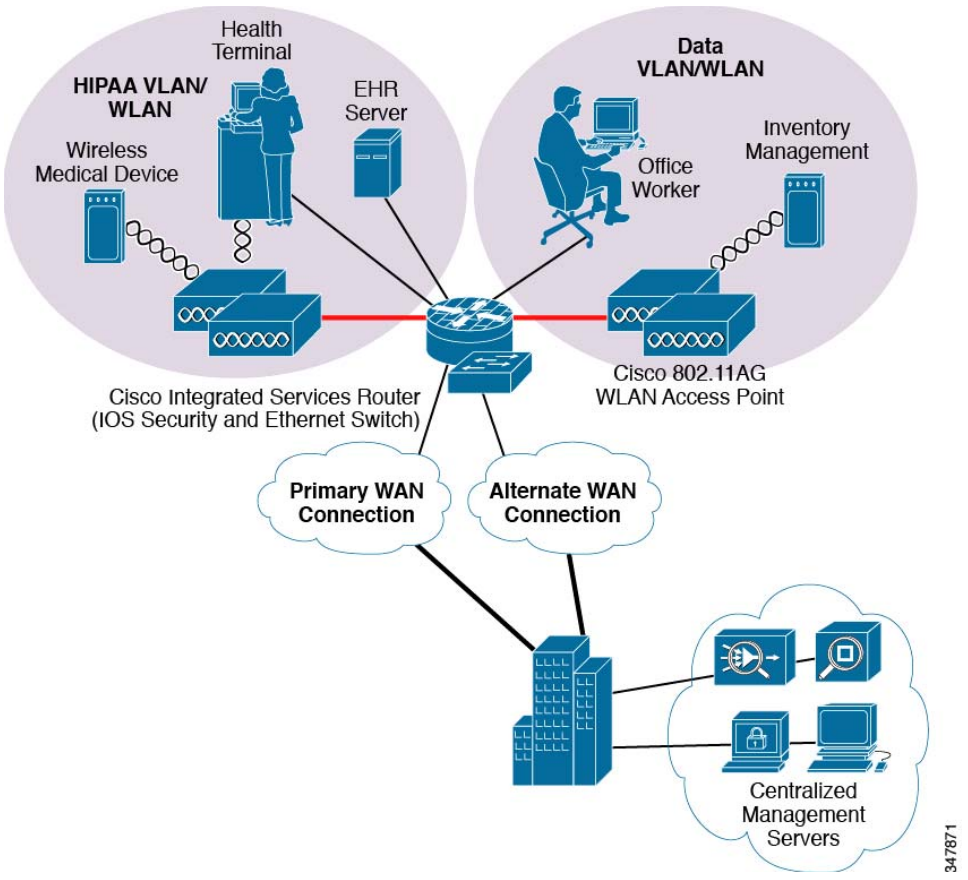
Note Each of these designs includes a variety of components that can be interchangeably used between them, depending on business requirements. For validation purposes, it was not necessary to implement all possible components in each design.

Small Clinic Architecture

Small clinics, such as a single physician or small physician practice, as shown in Figure 4-4, meet the following design requirements:

- Office size averages between 2000–6000 square feet; often the IT closet is outside of the control of the clinic in leased space, or is shared with other tenants. Often there is only one entry/exit and a fire door as an emergency escape, with remote or landlord-provided monitoring for fire and hazard controls.
- Fewer than 25 devices requiring network connectivity; many devices are standalone with widely variable networking and support requirements.
- Single router and integrated Ethernet switch.
- Preference for integrated services within fewer network components because of physical space requirements.
- Wireless connectivity for physician tablets and laptops to support physician mobility between treatment rooms.
- Treatment rooms and administrative offices designed to support specific clinical or administrative functions.
- Desire on the part of the physician to improve treatment options with advanced technology, but the need to control costs and make use of shared technology options such as video conferencing, remote audio dictation, and remote review of local medical instrumentation.

Figure 4-4 Small Clinic Architecture



The small clinic reference architecture is a powerful and modular platform for running multiple parallel and independent healthcare practices, all operating under a common operational and technical infrastructure. The small clinic module dictates simplicity and a compact form factor. This combination appeals to many clinical formats that can include the following:

- Traditional single doctor offices
- Small physician practices with 2–5 treatment rooms and basic functional organization
- Health specialty clinics and out-patient treatment facilities, designed specifically for one specialty —cancer treatment, OB/GYN, optical care, and out-patient surgical procedures, and so on
- Standardized clinic models running under a common “clinic” model—emergency care clinics, rehabilitation facilities, and so on

This network architecture is modular and consolidates many services into few infrastructure components. It supports a variety of clinic application models because an integrated Ethernet switch supports high-speed LAN services. Clinics routinely have minimal space for the technology infrastructure. The ability to implement the technological components securely in minimal space is an advantage.

Advantages include the following:

- Lower cost per site
- Fewer parts to spare, less complex remote maintenance required
- Less need to update software with fewer software images
- Lower equipment maintenance costs

Limitations include the following:

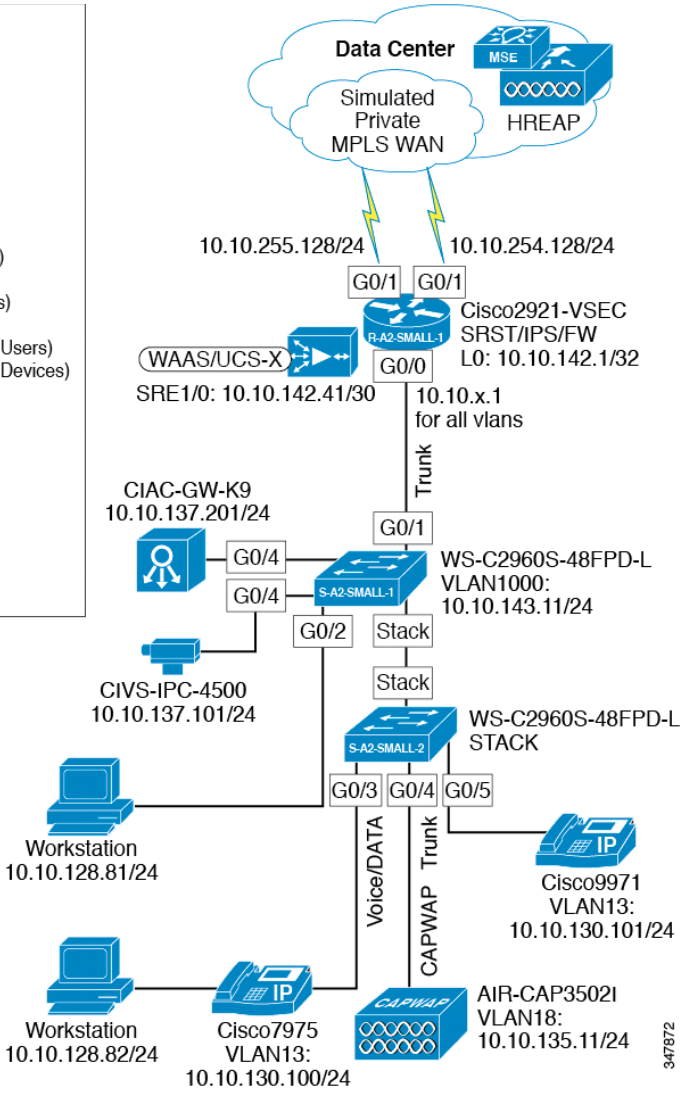
- Compromises in network resilience commensurate with the priority of treatment
- Some potential downtime because of single points of failure, demanding local replacement support

Small Clinic Design

Figure 4-5 shows the small clinic network design.

Figure 4-5 Small Clinic

IP Subnets	
10.10.128.0 255.255.240.0	**Small Aisle 2**
10.10.128.0 /24	VLAN11 (POS)
10.10.129.0 /24	VLAN12 (Data)
10.10.130.0 /24	VLAN13 (Voice)
10.10.131.0 /24	VLAN14 (Wireless)
10.10.132.0 /24	VLAN15 (Wireless POS)
10.10.133.0 /24	VLAN16 (Partner)
10.10.134.0 /24	VLAN17 (Wireless Guest)
10.10.135.0 /24	VLAN18 (Wireless Control)
10.10.136.0 /24	VLAN19 (WAE)
10.10.137.0 /24	VLAN20 (Security Systems)
10.10.138.0 /24	VLAN21 (HIPAA)
10.10.139.0 /24	VLAN22 (Wireless HIPAA-Users)
10.10.140.0 /24	VLAN23 (Wireless HIPAA-Devices)
10.10.141.0 /24	Other- (Misc)
10.10.142.0 /24	R-A2-Small-1 Loop 0
10.10.142.1 /32	(Future)
10.10.142.16 /30	(Future)
10.10.142.20 /30	(Future)
10.10.142.24 /30	(Future)
10.10.142.28 /30	VLAN 110 (SRE-SM)
10.10.142.32 /29	VLAN 111 (SRE-SM)
10.10.142.40 /30	VLAN1000 (Management)
10.10.143.0 /24	



Components Required

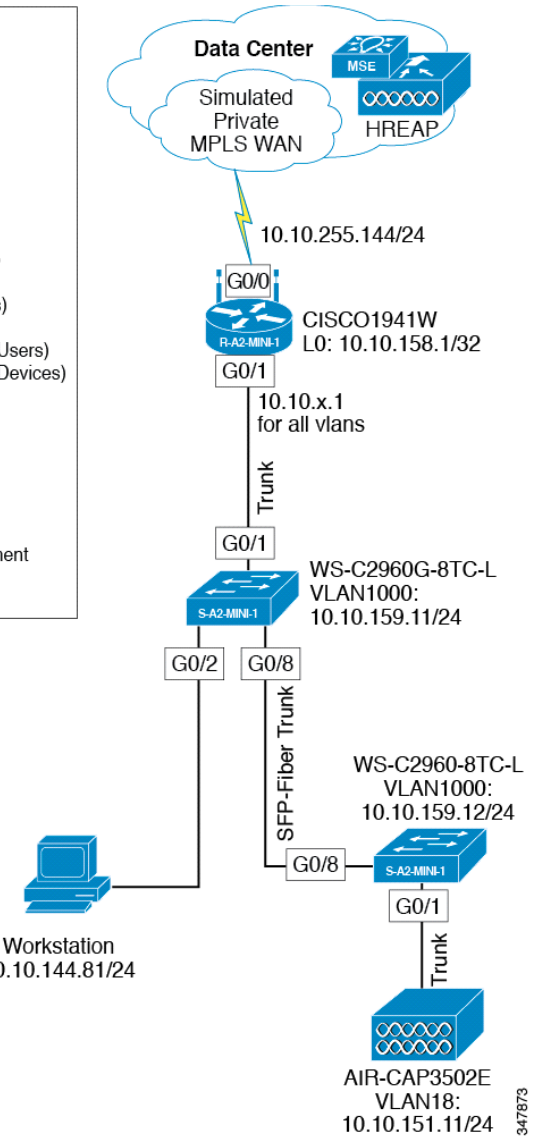
- Cisco 2921 Integrated Services Router (ISR)
- Cisco Catalyst 2960S 48-port PoE switch
- Cisco Aironet 3502i Access Points
- Cisco Video Surveillance 4500 Series IP Cameras
- Cisco Physical Access Gateway

Small Clinic—Mini Design

The mini clinic represents an alternate design for the small architecture, using different components. Figure 4-6 shows the mini clinic network design.

Figure 4-6 Mini Clinic Network Design

IP Subnets	
10.10.144.0 255.255.240.0	**Mini Aisle 2**
10.10.144.0 /24	VLAN11 (POS)
10.10.145.0 /24	VLAN12 (Data)
10.10.146.0 /24	VLAN13 (Voice)
10.10.147.0 /24	VLAN14 (Wireless)
10.10.148.0 /24	VLAN15 (Wireless POS)
10.10.149.0 /24	VLAN16 (Partner)
10.10.150.0 /24	VLAN17 (Wireless Guest)
10.10.151.0 /24	VLAN18 (Wireless Control)
10.10.152.0 /24	VLAN19 (WAE)
10.10.153.0 /24	VLAN20 (Security Systems)
10.10.154.0 /24	VLAN21 (HIPAA)
10.10.155.0 /24	VLAN22 (Wireless HIPAA-Users)
10.10.156.0 /24	VLAN23 (Wireless HIPAA-Devices)
10.10.157.0 /24	Other- (Misc)
10.10.158.0 /24	R-A2-Mini-1 Loop 0
10.10.158.1 /32	(Future)
10.10.158.16 /30	(Future)
10.10.158.20 /30	(Future)
10.10.158.24 /30	(Future)
10.10.158.28 /30	VLAN 110 (Wireless NM)
10.10.158.32 /29	VLAN 111 (WAE Management
10.10.158.40 /30	VLAN1000 (Management)
10.10.159.0 /24	



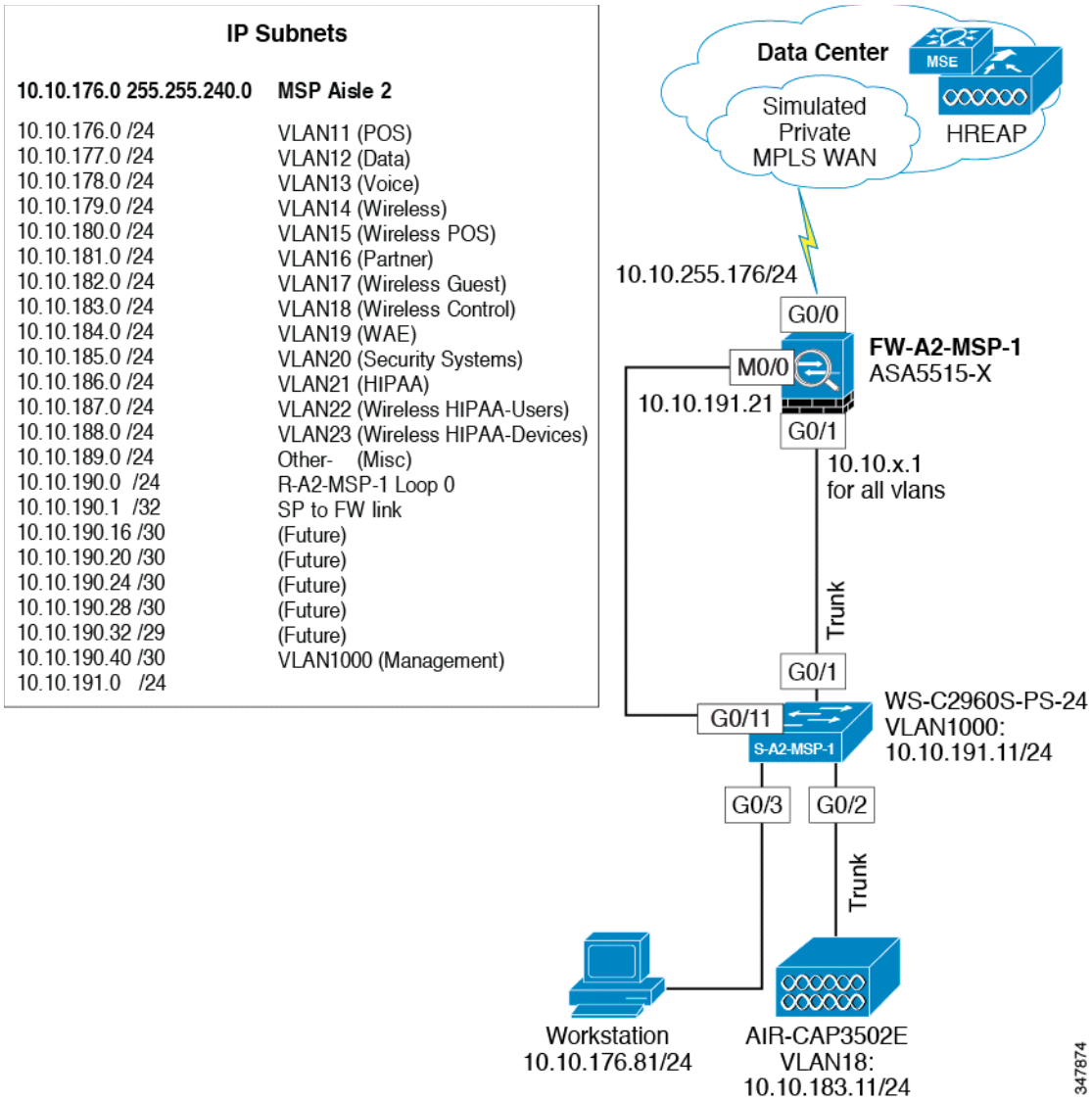
Components Selected

- Cisco 1941 Integrated Services Router (ISR)
- Cisco Catalyst 2960 Switch
- Cisco Aironet 3502e Access Point

Small Clinic—Managed Service Provider Design

The managed service provider office represents an alternate design for the small clinic architecture. Figure 4-7 shows the managed service provider network design.

Figure 4-7 Managed Service Provider Office Network Design



Components Selected

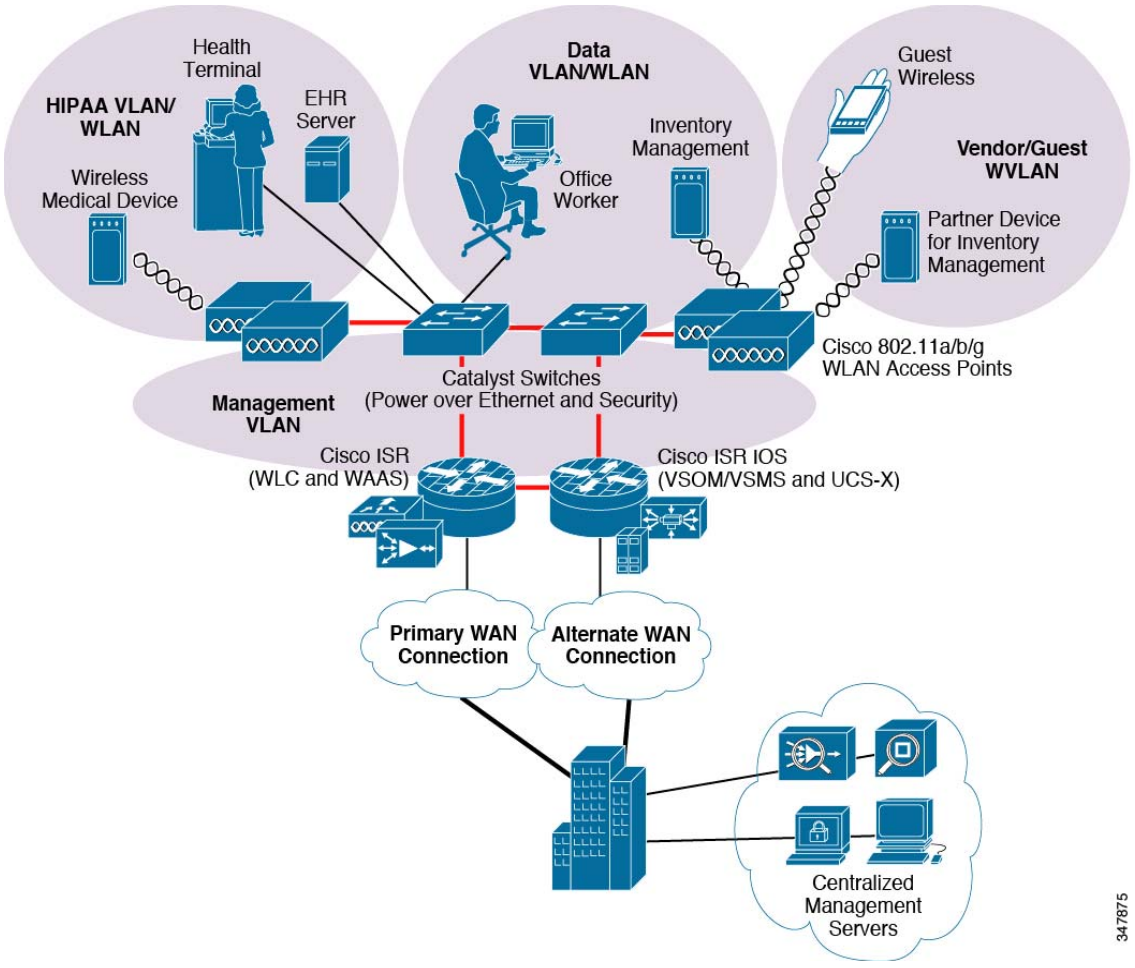
- Cisco ASA 5515-x Firewall with vIPS
- Cisco Catalyst 2960S Switch
- Cisco Aironet 3502e Access Points

Medium Clinic Architecture

Medium clinics such as a physician practice or multi-practice, shown in Figure 4-8, meet the following design requirements:

- Facility space between 5000 and 30000 square feet with one of more floors of dedicated office and clinic spaces, waiting rooms, purpose-built treatment rooms, storage facilities of various types, and dedicated IT and utility spaces
- Number of devices connecting to the network averages 25–100 devices with most requiring IP network connectivity, and providing integrated telephone switching/call routing throughout the facility
- Redundant LAN and WAN infrastructures, and more purpose-specific devices for greater control and flexibility
- Wireless connectivity for mobile carts and wireless medical devices to support physician mobility between treatment rooms and review of patient data
- Treatment rooms and administrative offices designed to support specific clinical or administrative functions

Figure 4-8 Medium Clinic Architecture



The medium clinic architecture provides for flexibility to support a wide range of clinic operations under a common and cost-effective networking model. This model stresses the adaptability of the architecture to multiple functions and data types, all brought under a common control structure so the healthcare security requirements can be controlled either at the clinic or centrally across the larger organization. The medium clinic architecture is optimized for efficient business operation without sacrificing centralized controls and layered security control to best resist breach.

Owing to the flexibility of the architecture, the medium clinic model can be adapted to many configurations of out-patient clinics and today's small hospitals.

The reference architecture is designed for clinical operations that require network resiliency and increased levels of application availability over the small clinic architecture and its single-threaded, simple approach. As more mission-critical applications and services converge onto the IP infrastructure, network uptime and application availability are more important. The dual-router and dual-LAN switch design of the medium clinic supports these requirements. Each of the ISR routers can run Cisco IOS security services and other clinic communication services simultaneously. Each of the Cisco ISR routers is connected to a dedicated WAN connection. Hot-Standby Routing Protocol (HSRP) is used to ensure network resilience in the event that the network connection fails.

The access layer of the network offers enhanced levels of flexibility and more access ports compared to the small clinic. Up to 12 wireless access points can be installed in the clinic, supported by the Cisco Wireless LAN Controller (WLC) as tested and without adding more controllers. The distributed Cisco Catalyst switches can support a combination of larger physical buildings or a larger number of endpoints than the small clinic.

Advantages include the following:

- More adaptive access layer with support for a greater number of endpoints and more diverse building requirements (multiple floors, sub-areas, and so on)
- Improved network resilience through parallel device design
- Improved network and application availability through parallel paths

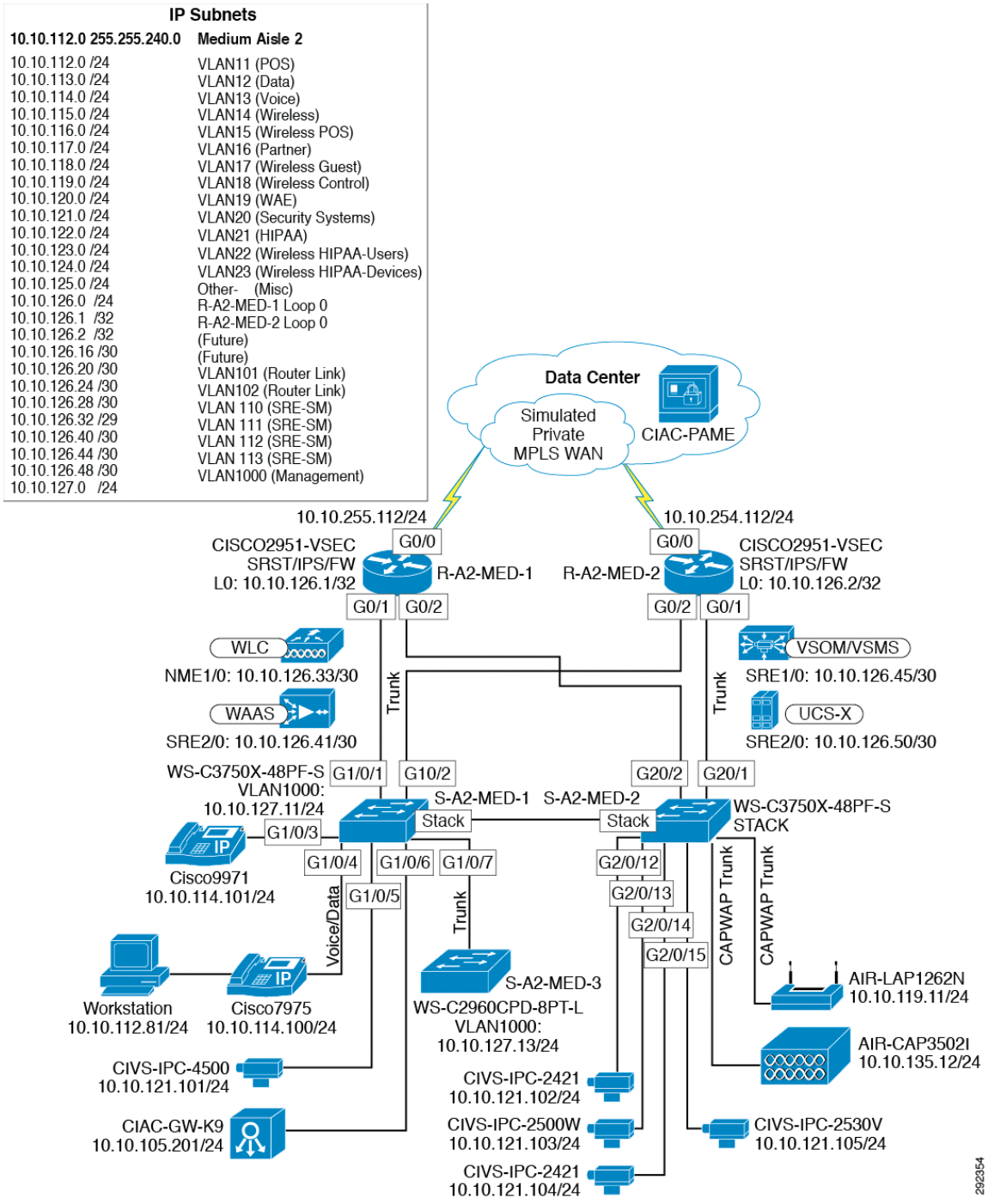
Limitations include the following:

- No distribution layer between core layer (the ISR) and the access layer switches
- A single WLC controller decreases in-clinic resilience of the wireless network; the recommendation is to have clinic APs fallback to the central WLC controller if the local WLC controller fails, or to install dual-local WLC controllers.

Medium Clinic Design

Figure 4-9 shows the medium clinic design.

Figure 4-9 Medium Clinic Design



Components Selected

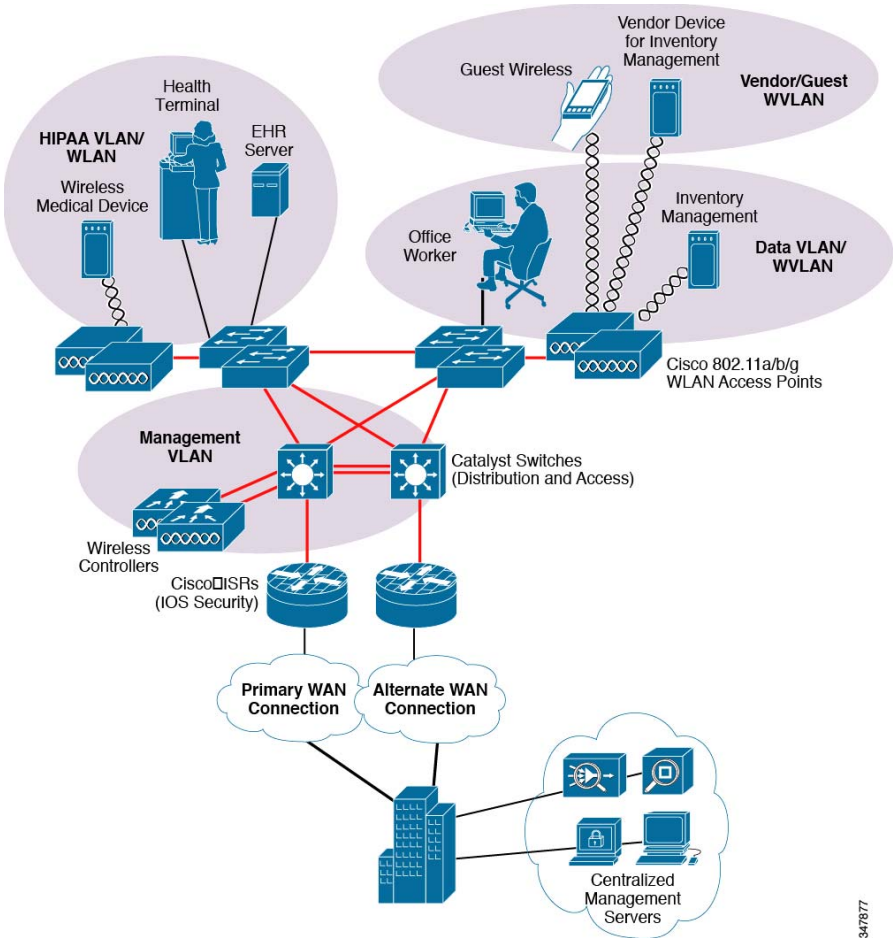
- Cisco 2951 Integrated Services Router (ISR)
- Cisco Catalyst 3750X 48-port PoE Switch
- Cisco Catalyst 2960 Compact Switch
- Cisco Aironet 3502e and 1262N Access Points
- Cisco Video Surveillance 2421 IP Dome Camera
- Cisco Video Surveillance 2500 Series IP Camera
- Cisco Operations Manager v4.1
- Cisco Physical Access Gateway

Hospital Architecture

The hospital reference architecture model shown in Figure 4-10 meets the following design requirements:

- Facility space between 3,000 to 3,000,000 square feet with one of more floors of dedicated office and clinic spaces, waiting rooms, purpose-built treatment rooms, storage facilities of various types, and dedicated IT and utility spaces
- Number of devices connecting to the network averages 250–1000 devices with most requiring IP network connectivity, and providing integrated telephone switching/call routing throughout the facility
- Redundant LAN and WAN infrastructures, and more purpose-specific devices for greater control and flexibility
- Large capacity network infrastructure to support high bandwidth demands for imaging, video conferencing, and telemedicine
- Wireless connectivity for mobile carts and wireless medical devices to support physician mobility between treatment rooms and review of patient data on laptops, tablets, and specialty devices
- Unified communications integration for current and future needs including VoIP, calling stations, IPTV, web conferencing, video conferencing, and telemedicine
- Treatment rooms and administrative offices designed to support specific clinical or administrative functions

Figure 4-10 Hospital Architecture



The hospital reference architecture uses Cisco campus network architecture recommendations and adapts them to a healthcare environment. Network traffic can be better segmented (logically and physically) to meet business requirements. The distribution layer architecture can greatly improve LAN performance while offering enhanced physical media connections (that is, fiber and copper for connection to remote access layer switches and wireless access points). A larger number of endpoints can be added to the network to meet business requirements. Dual routers and distribution layer media flexibility greatly improve network serviceability because the network is highly available and scales to support the site requirements. Routine maintenance and upgrades can be scheduled and performed more frequently or during normal business hours because of parallel path design.

Advantages include the following:

- Highest network resilience based on highly available design
- Port density and fiber density for large locations
- Increase segmentation of traffic
- Scalable to accommodate shifting requirements

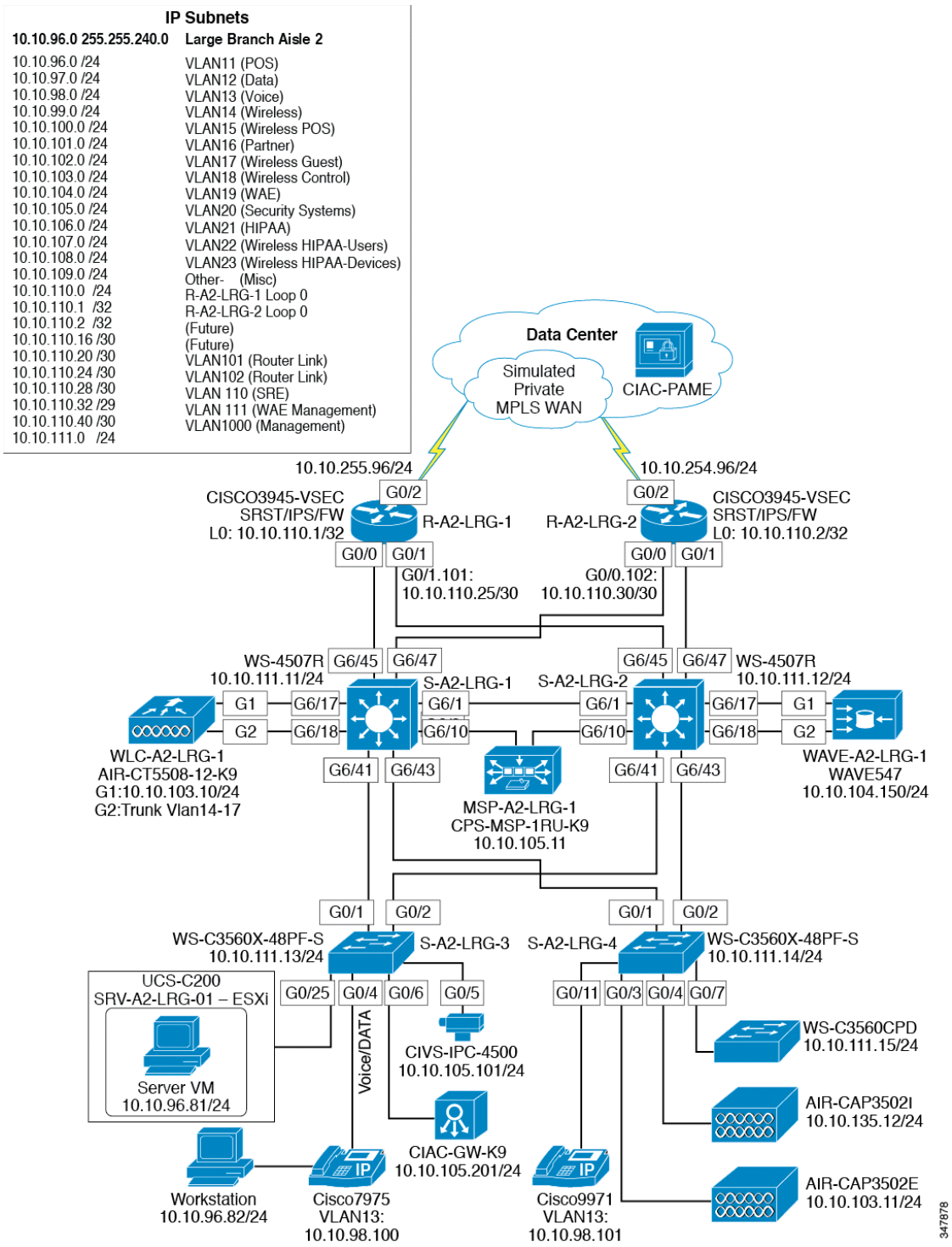
Limitations include the following:

- Higher cost because of network resilience based on highly available design
- These network designs are capable of helping an organization achieve compliance, and also serve as the scalable platform for new services and applications

Hospital Design

Figure 4-11 shows the hospital network design.

Figure 4-11 Hospital Network Design



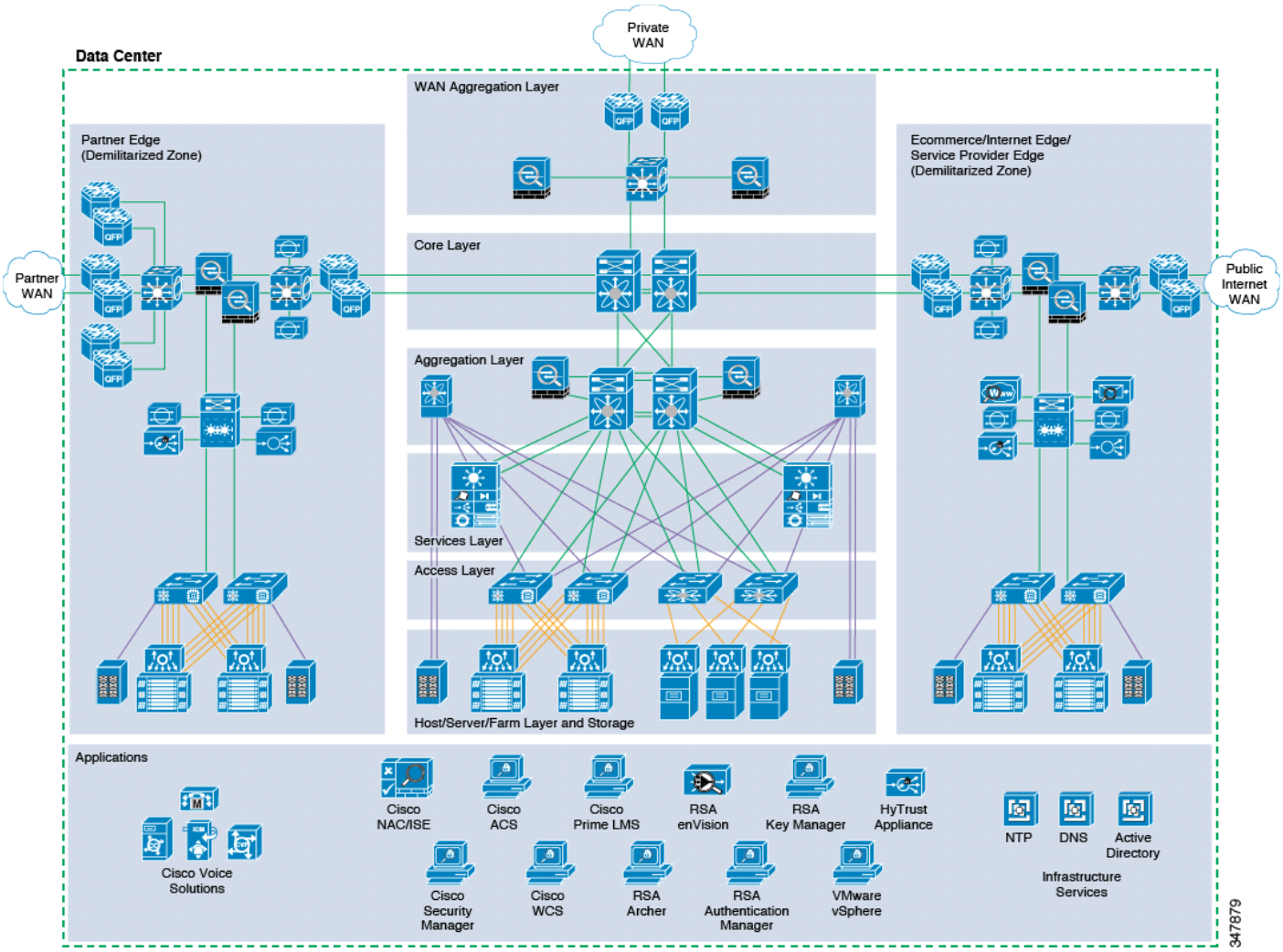
Components Selected

- Cisco 3945 Integrated Services Router (ISR)
- Cisco Catalyst 3560X and 4500 switches
- Cisco Aironet 3502e and 3502i Access Points
- Cisco 5508 Wireless Controller
- Cisco 4500 Video Surveillance Camera
- Cisco Physical Access Gateway

Data Center

The data center is where centralized data communications occur and are stored (see Figure 4-12). The data center is also the place where management systems are deployed. The data center provides centralized control from an administrative perspective because it is typically where the tools that are used to monitor and enforce compliance are deployed.

Figure 4-12 Data Center Architecture



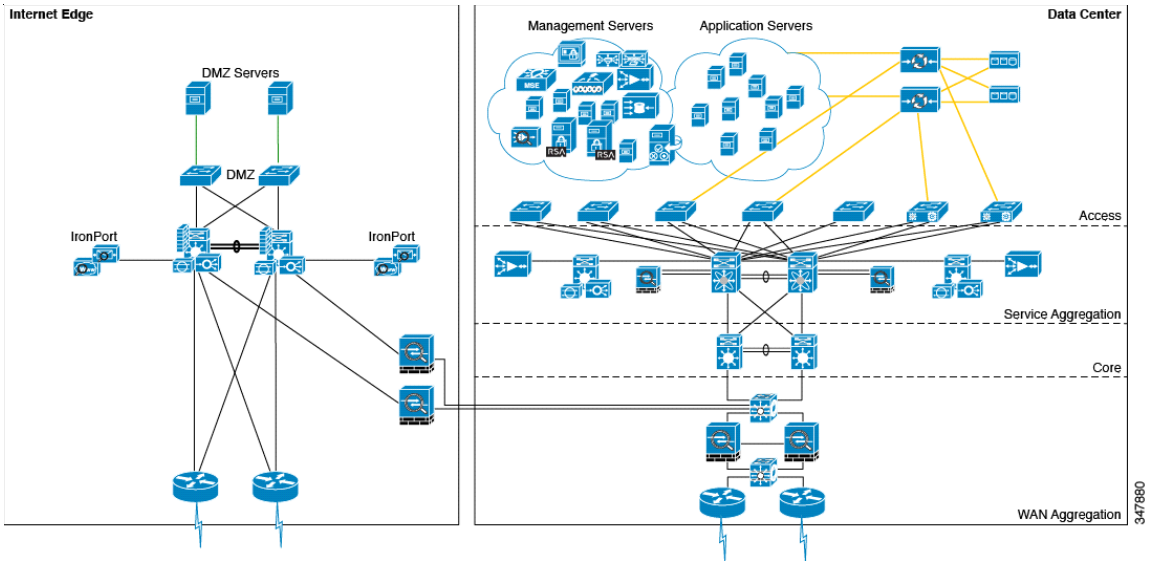
Design considerations are as follows:

- Centralized solution management supports all aspects of network, security, and systems management; and supports remote access from anywhere on the network.
- Standardized equipment and software images, deployed in a modular, layered approach, simplify configuration management and increase the systems availability.
- The highly available data center design permits highly resilient access from clinics to core data and storage services.
- WAN aggregation alternatives allow flexible selection of service provider network offerings.

- The service aggregation design allows for a modular approach to adding new access layers and managing shared network services (for example, firewall, IDS, application networking, wireless management).
- Firewall, IDS, and application networking services are available at the service and aggregation layers of the data center.
- Scalability to accommodate shifting requirements in data center compute and storage requirements.
- WAN access speeds are typically the limiting factor between the clinic network systems and the WAN aggregation layer.
- It is typical for implementers to over-subscribe the WAN circuits between the clinics and the WAN edge aggregation router. Over-subscription can cause inconsistent results and packet loss of PHI in the event that more traffic enters the WAN circuit simultaneously.
- Backup network connections from clinic networks to the data center are recommended when PHI is transported via the WAN.

Figure 4-13 shows the data center design.

Figure 4-13 Data Center Design



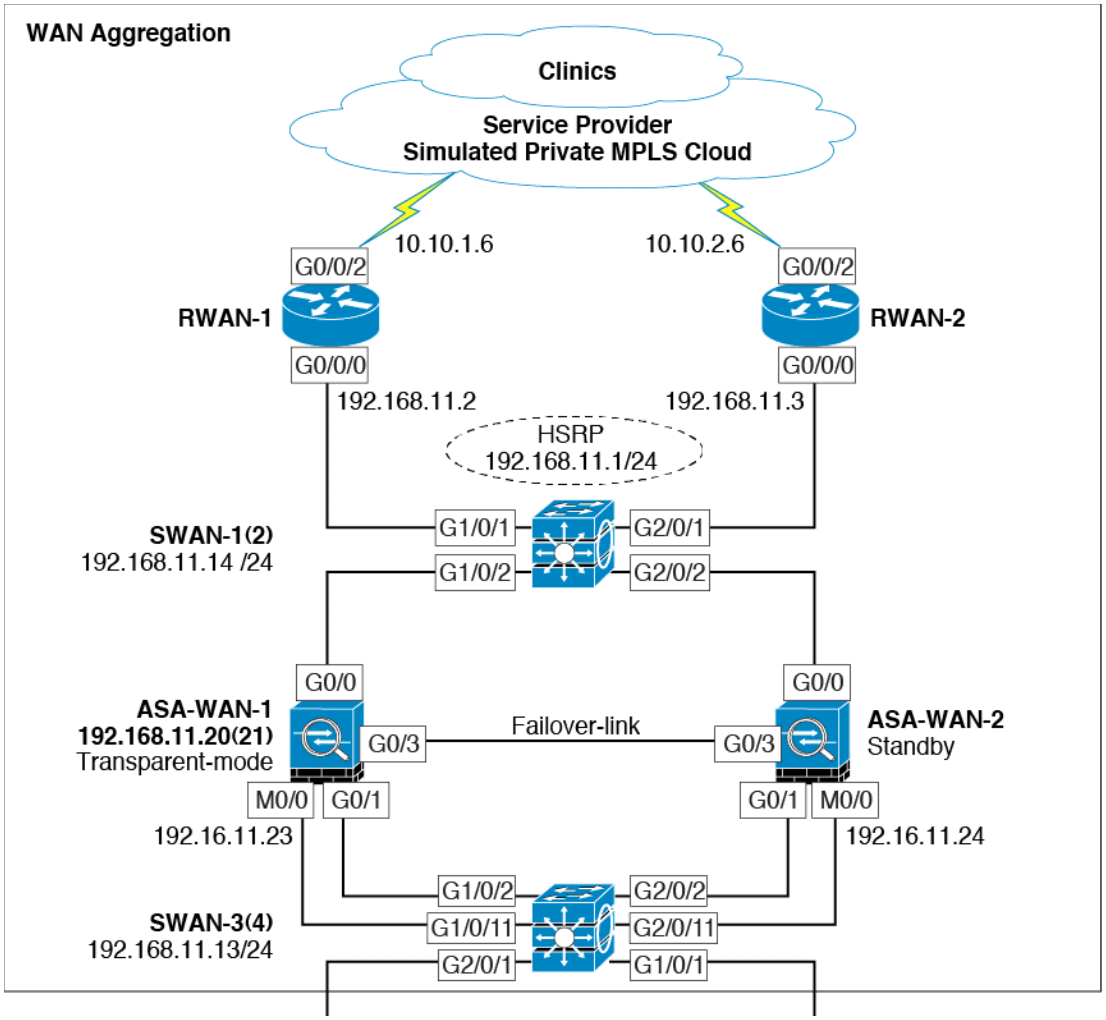
Data centers can house many types of functions, and the term itself can encompass narrow and broad aspects. For the purposes of this guide, data centers include the following functions:

- WAN aggregation layer—Aggregates the clinic and backstage WAN connections to the core
- Core layer—Highly available, high-speed area that is the central point of connectivity to all data center areas
- Aggregation block—Aggregates the services of one area and connects that area to the core, including Vblock1 design
- Internet edge—Secure connectivity to the Internet

WAN Aggregation Layer

Figure 4-14 shows the WAN aggregation layer design.

Figure 4-14 WAN Aggregation Layer Design



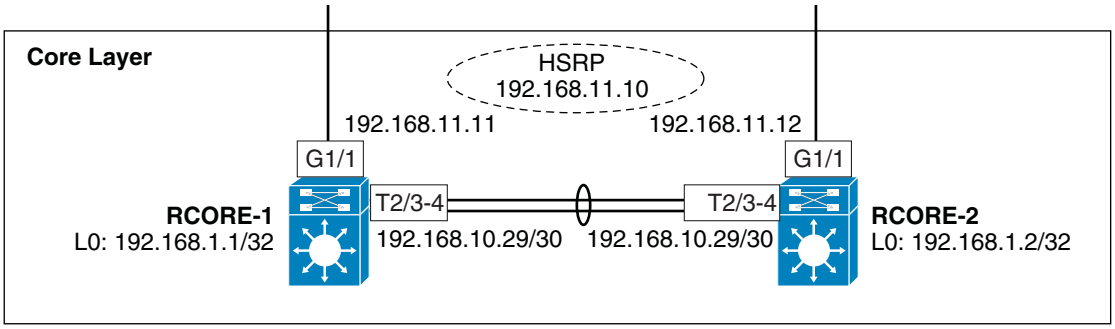
Components Selected

- Cisco ASR 1002-Fixed Router
- Cisco ASA 5555-X Adaptive Security Appliance
- Cisco Catalyst 3750X Switch

Core Layer Design

Figure 4-15 shows the core layer design.

Figure 4-15 Core Layer Design



Components Selected

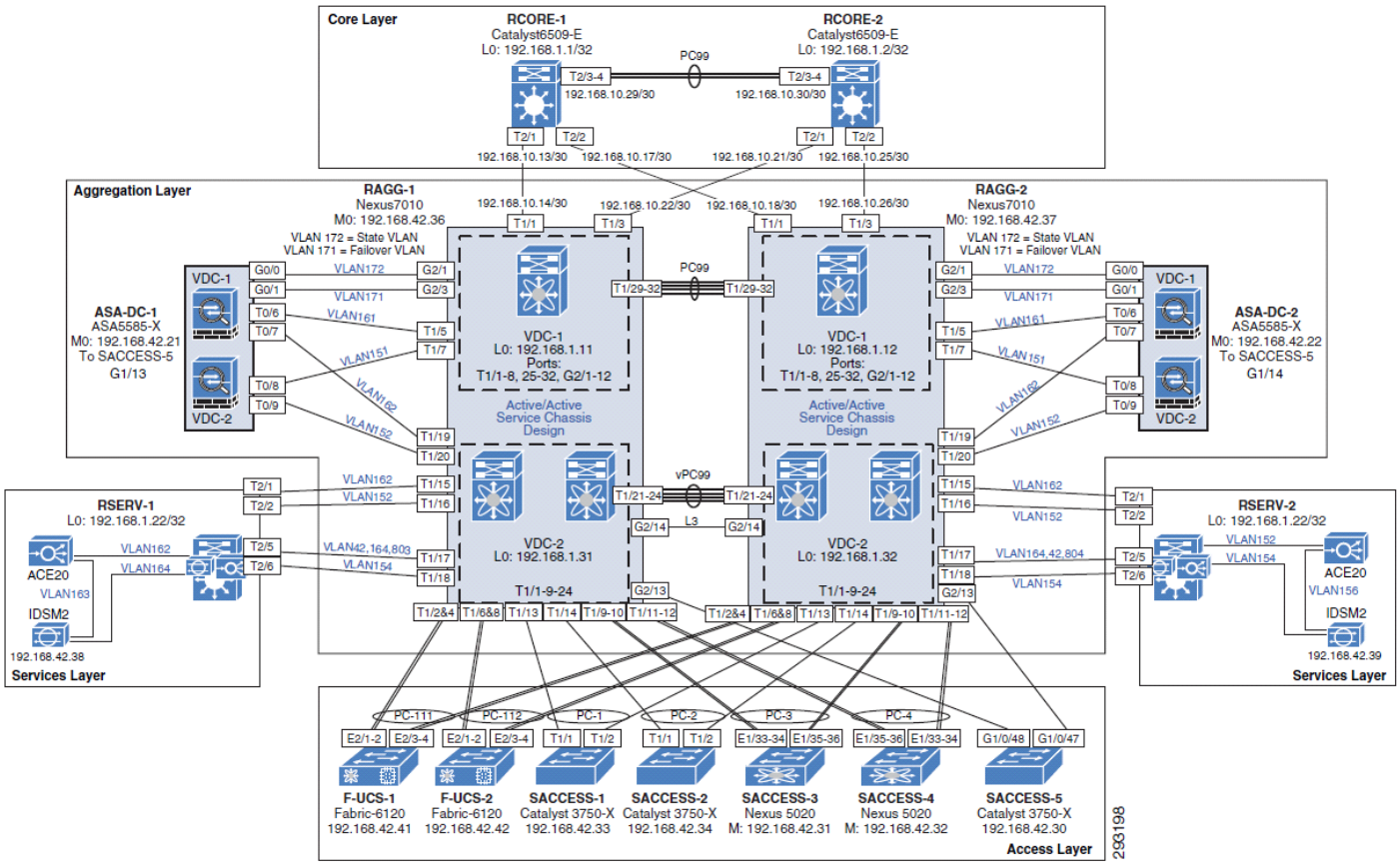
- Cisco Catalyst 6500-E Switch

Note In Chapter 3, "Solution Architecture," the Cisco Nexus switch is recommended as the core layer component. At the time of this solution validation, the Cisco Catalyst was used in the core switching layer.

Aggregation Block Design

Figure 4-16 shows the aggregation block design.

Figure 4-16 Aggregation Block Design



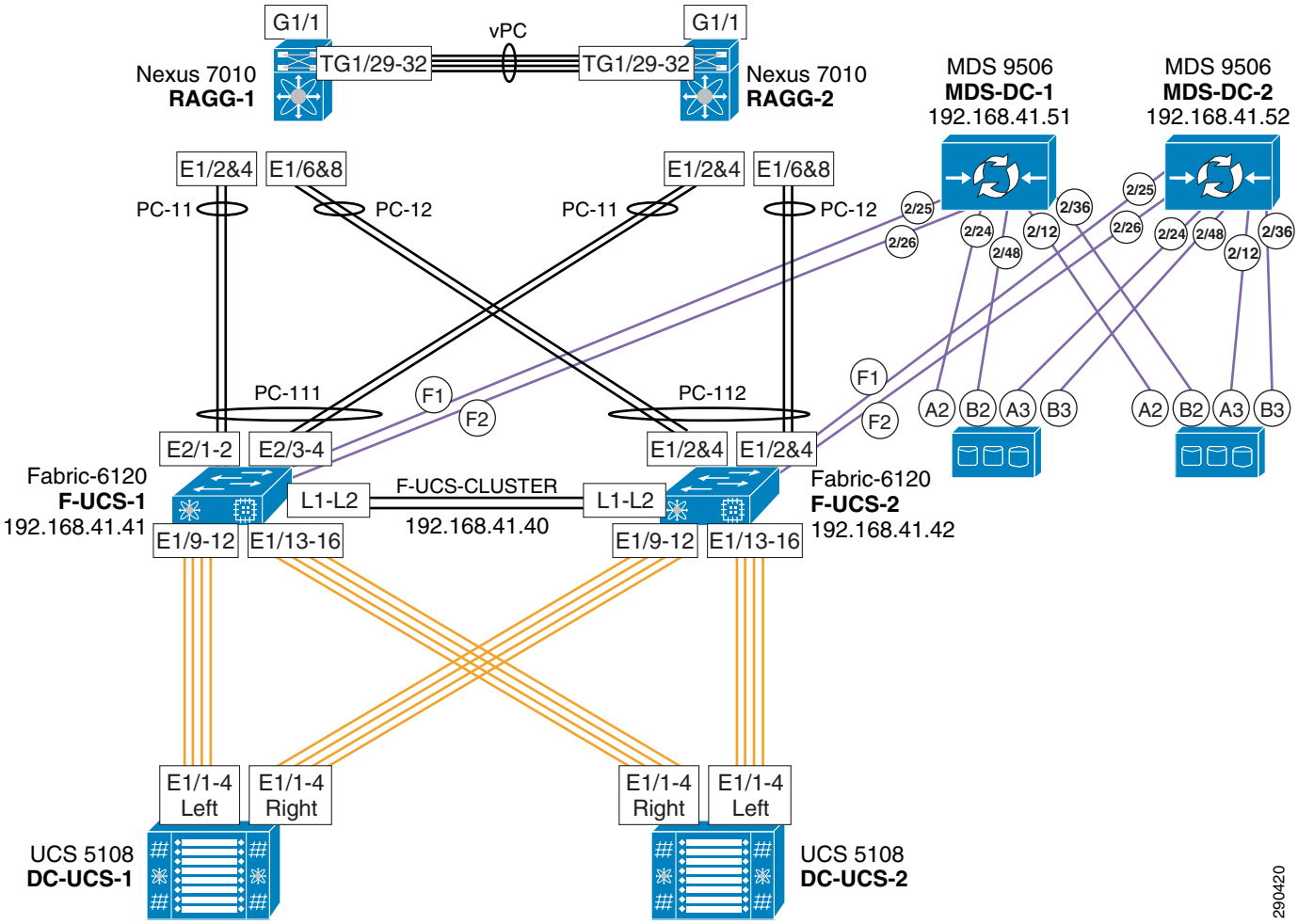
Components Selected

- Cisco ASA 5585-X Adaptive Security Appliance
- Cisco Nexus 7010 Switch
- Cisco Catalyst 6500-E Switch
  - Cisco ACE 20
  - Cisco IDSM-2
- Cisco Nexus 5020 Switch
- Cisco Catalyst 3750-X Switch

Vblock Design

Figure 4-17 shows the Vblock design.

Figure 4-17 Vblock Design



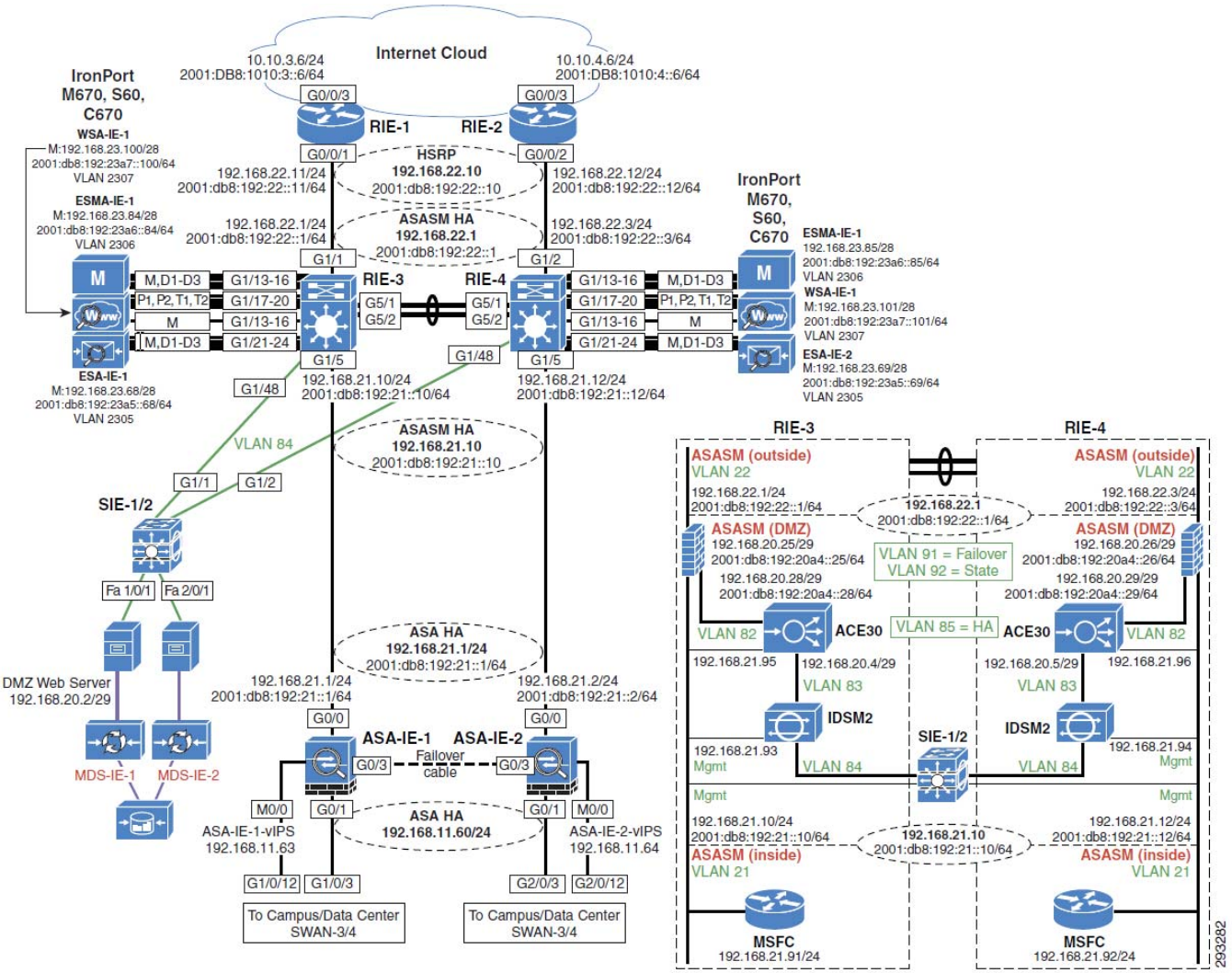
Components Selected

- Cisco UCS 5108 Blade Server Chassis
  - Cisco B200 Blade
- Cisco UCS 6120 Fabric Interconnect
- Cisco MDS 9506 Multilayer Director
- EMC CLARiion CX4 Model 240

Internet Edge Design

Figure 4-18 shows the Internet edge design.

Figure 4-18 Internet Edge Design



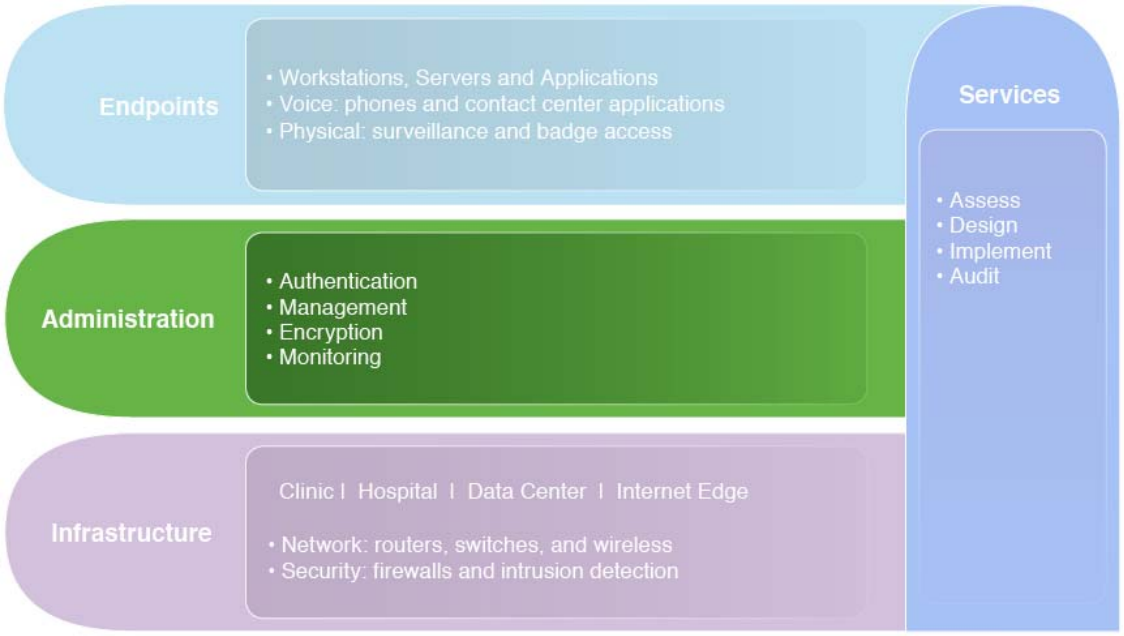
Components Selected

- Cisco ASR 1002 Series Router
- Cisco Catalyst 6500-E Switch
  - Cisco ASASM
  - Cisco ACE 30
  - Cisco IDSM-2
- Cisco Catalyst 3750X Switch
- Cisco MDS 9204i Switch
- Cisco IronPort C670

Administration

The administration layer of the solution framework addresses the components such as authentication, encryption, management, and monitoring, as shown in Figure 4-19.

Figure 4-19 Scope Administration Layer of the Solution Framework



Authentication

Components Selected

- Cisco Secure Access Control Server (ACS)
- Cisco Identity Services Engine (ISE)
- RSA Authentication Manager
- Windows Active Directory

PHI Encryption

Components Selected

- Cisco Security Manager
- Cisco Key Manager
- Cisco AnyConnect VPN
- RSA Data Protection Manager

Management

Components Selected

- Cisco Prime LAN Management Solution (LMS)
- Cisco Security Manager
- Cisco Wireless Control Server Manager
- EMC Unified Infrastructure Manager
- VMware vSphere vCenter
- Cisco Video Surveillance Manager
- Cisco Physical Access Manager
- RSA Archer

Monitoring

Components Selected

- RSA enVision
- HyTrust

Endpoints and Applications

The endpoints and applications layer of the solution framework addresses the components such as voice and physical security, as shown in Figure 4-20.

Figure 4-20 Endpoints and Applications Layer of the PHI Solution Framework

Physical

Components Selected

- Cisco Physical Access Gateway
- Cisco Video Surveillance Cameras (2421, 2500, 4500)

Voice

Components Selected

- Cisco Unified Communications Manager
- Cisco IP Phones (9971, 7975)
- Cisco Survivable Remote Site Telephony (SRST)

Services

The right-hand element that spans endpoint, administration, and infrastructure layers includes services to plan, build, and manage the network to address the HIPAA Security Rule. These can be provided by Cisco, Cisco partners, and Verizon Business. Sample services can include the following:

- Strategy and analysis
- Assessments
- Design
- Validation
- Deployment
- Migration
- Product and solution support
- Optimization and operation services

Note For a complete Bill of Materials, see Appendix A, "Bill Of Material." For assessment of components selected for PHI compliance, see Chapter 5, "Component Assessment." For complete running configurations of components, see Appendix E, "Detailed Full Running Configurations."

Cisco Compliance Solution for HIPAA Security Rule Result Summary

This solution combines components to create an end-to-end solution conforming to the security controls requirements as outlined in the HIPAA Security Rule Safeguards (see Table 4-1). The result is a set of recommended clinic, hospital, data center, and Internet-edge architectures and designs that can simplify the process of developing and maintaining healthcare security controls in support of a risk management program as required by HIPAA.

Table 4-1 HIPAA Safeguards Supported

Endpoints	HIPAA Safeguards Supported
Cisco Physical Access Manager/Gateway	Security Management Process: • 164.308(a)(1)(i) Security Management Process Physical Access, IDS, Surveillance: • 164.310(a)(1) Physical Access Control Identity/Authorization/Access Control: • 164.308(a)(3)(ii)(A) Authorization/Supervision • 164.308(a)(3)(ii(C)) Termination Procedures • 164.308(a)(4)(ii)(B) Access Authorization • 164.308(a)(4)(ii)(C) Access Est./ Modification
Cisco UCS and UCS Express	• 164.308(a)(1)(i) Security Management Process • 164.308(a)(3)(ii)(A) Authorization/Supervision • 164.308(a)(4)(ii)(A) Isolating Clearinghouse Functions • 164.308(a)(5)(i) Log-in Monitoring • 164.308(a)(6)(i) Security Incident Procedures • 164.308(a)(6)(ii) Response and Reporting • 164.312(a)(i) Access Control • 164.312(b) Audit Controls • 164.312(c)(1) Data Integrity
Administration	

Table 4-1 HIPAA Safeguards Supported (continued)

CISCO ACS	• 164.308(a)(1)(i) Security Management Process • 164.308(a)(3)(ii)(A) Authorization/Supervision • 164.308(a)(4)(ii)(B) Access Authorization • 164.308(a)(4)(ii)(C) Access Establishment and Modification • 164.308(a)(5)(i) Log-in Monitoring • 164.308(a)(6)(i) Security Incident Procedures • 164.308(a)(6)(ii) Response and Reporting • 164.312(a)(2)(i) Unique User Identification • 164.312(a)(2)(ii) Emergency Access Procedures • 164.312(b) Audit Controls • 164.312(d) Person or Entity Authentication
Cisco Identity Services Engine	• 164.308(a)(1)(i) Security Management Process • 164.308(a)(3)(ii)(A) Authorization/Supervision • 164.308(a)(4)(ii)(B) Access Authorization • 164.308(a)(4)(ii)(C) Access Establishment and Modification • 164.308(a)(5)(i) Log-in Monitoring • 164.308(a)(5)(ii)(D) Password Management • 164.308(a)(6)(i) Security Incident Procedures • 164.308(a)(6)(ii) Response and Reporting • 164.312(a)(i) Access Control • 164.312(b) Audit Controls • 164.312(a)(2)(ii) Emergency Access Procedures • 164.312(a)(d) Person or Entity Authentication
Cisco Prime LMS	• 164.308(a)(1)(i) Security Management Process • 164.308(a)(3)(ii)(A) Authorization/Supervision • 164.308(a)(4)(ii)(B) Access Authorization • 164.308(a)(5)(i) Log-in Monitoring • 164.308(a)(6)(ii) Response and Reporting • 164.312(a)(i) Access Control • 164.312(b) Audit Controls

Table 4-1 HIPAA Safeguards Supported (continued)

Cisco Security Manager	• 164.308(a)(1)(i) Security Management Process • 164.308(a)(3)(ii)(A) Authorization/Supervision • 164.308(a)(4)(ii)(B) Access Authorization • 164.308(a)(4)(ii)(C) Access Establishment and Modification • 164.308(a)(5)(i) Log-in Monitoring • 164.308(a)(5)(ii)(D) Password Management • 164.308(a)(6)(ii) Response and Reporting • 164.312(a)((2)(i) Unique User Identification • 164.312(b) Audit Controls • 164.312(a)(d) Person or Entity Authentication
HyTrust Enterprise	• 164.308(a)(1)(i) Security Management Process • 164.308(a)(3)(ii)(A) Authorization/Supervision • 164.308(a)(4)(ii)(B) Access Authorization • 164.308(a)(5)(i) Log-in Monitoring • 164.308(a)(6)(ii) Response and Reporting • 164.312(a)(i) Access Control • 164.312(b) Audit Controls
RSA Authentication Manager	• 164.308(a)(1)(i) Security Management Process • 164.308(a)(3)(ii)(A) Authorization/Supervision • 164.308(a)(4)(ii)(B) Access Authorization • 164.308(a)(4)(ii)(C) Access Establishment and Modification • 164.308(a)(5)(i) Log-in Monitoring • 164.308(a)(5)(ii)(D) Password Management • 164.308(a)(6)(i) Security Incident Procedures • 164.308(a)(6)(ii) Response and Reporting • 164.312(a)(i) Access Control • 164.312(b) Audit Controls • 164.312(a)(2)(ii) Emergency Access Procedures • 164.312(a)(d) Person or Entity Authentication Security Management Process: • 164.308(a)(1)(i) Security Management Process Logging/Auditing/Monitoring: • 164.308(a)(1)(ii)(D) Information System Activity Review

Table 4-1 HIPAA Safeguards Supported (continued)

RSA Protection Manager	• 164.308(a)(1)(i) Security Management Process • 164.308(a)(3)(ii)(A) Authorization/Supervision • 164.308(a)(4)(ii)(B) Access Authorization • 164.308(a)(5)(i) Log-in Monitoring • 164.308(a)(6)(i) Security Incident Procedures • 164.312(a)(i) Access Control • 164.312(b) Audit Controls • 164.312(c)(1) Data Integrity
RSA enVision	• 164.308(a)(1)(i) Security Management Process • 164.308(a)(1)(ii)(D) Information System Activity Review • 164.308(a)(3)(ii)(A) Authorization/Supervision • 164.308(a)(5)(i) Log-in Monitoring • 164.308(a)(6)(ii) Response and Reporting • 164.312(b) Audit Controls
Infrastructure	
Cisco ASA Branch	• 164.308(a)(1)(i) Security Management Process • 164.308(a)(4)(ii)(A) Isolating health care clearinghouse function • 164.308(a)(4)(ii)(B) Access Authorization • 164.308(a)(4)(ii)(C) Access Establishment and Modification • 164.308(a)(5)(i) Log-in Monitoring • 164.308(a)(6)(ii) Response and Reporting • 164.312(a)(i) Access Control • 164.312(a)(2)(i) Unique User Identification • 164.312(a)(2)(ii) Emergency Access procedures • 164.312(a)(2)(iii) Automatic Logoff • 164.312(a)(ii)(iv) Encryption and Decryption • 164.312(b) Audit Controls • 164.312(c)(1) Data Integrity • 164.312(d) Person or Entity Authentication • 164.312(e)(i) Transmission Security • 164.312(e)(2)(i) Integrity Controls • 164.312(e)(2)(ii) Encryption

Table 4-1 HIPAA Safeguards Supported (continued)

Cisco ASA Data Center	• 164.308(a)(1)(i) Security Management Process • 164.308(a)(4)(ii)(A) Isolating health care clearinghouse function • 164.308(a)(4)(ii)(B) Access Authorization • 164.308(a)(4)(ii)(C) Access Establishment and Modification • 164.308(a)(5)(i) Log-in Monitoring • 164.308(a)(6)(ii) Response and Reporting • 164.312(a)(i) Access Control • 164.312(a)(2)(i) Unique User Identification • 164.312(a)(2)(ii) Emergency Access procedures • 164.312(a)(2)(iii) Automatic Logoff • 164.312(a)(ii)(iv) Encryption and Decryption • 164.312(b) Audit Controls • 164.312(c)(1) Data Integrity • 164.312(d) Person or Entity Authentication • 164.312(e)(i) Transmission Security • 164.312(e)(2)(i) Integrity Controls • 164.312(e)(2)(ii) Encryption
Cisco Branch Routers	• 164.308(a)(1)(i) Security Management Process • 164.308(a)(4)(ii)(A) Isolating health care clearinghouse function • 164.308(a)(4)(ii)(B) Access Authorization • 164.308(a)(4)(ii)(C) Access Establishment and Modification • 164.308(a)(5)(i) Log-in Monitoring • 164.308(a)(6)(ii) Response and Reporting • 164.312(a)(i) Access Control • 164.312(a)(2)(i) Unique User Identification • 164.312(a)(2)(ii) Emergency Access procedures • 164.312(a)(2)(iii) Automatic Logoff • 164.312(a)(ii)(iv) Encryption and Decryption • 164.312(b) Audit Controls • 164.312(c)(1) Data Integrity • 164.312(d) Person or Entity Authentication • 164.312(e)(i) Transmission Security • 164.312(e)(2)(i) Integrity Controls • 164.312(e)(2)(ii) Encryption

Table 4-1 HIPAA Safeguards Supported (continued)

Cisco Branch Switches	• 164.308(a)(1)(i) Security Management Process • 164.308(a)(3)(i) Authorization/Supervision • 164.308(a)(4)(ii)(B) Access Authorization • 164.308(a)(5)(i) Log-in Monitoring • 164.308(a)(6)(ii) Response and Reporting • 164.312(a)(i) Access Control • 164.312(b) Audit Controls • 164.312(c)(1) Data Integrity • 164.312(e)(i) Transmission Security • 164.312(e)(2)(i) Integrity Controls • 164.312(e)(2)(ii) Encryption
Cisco Data Center Routers	• 164.308(a)(1)(i) Security Management Process • 164.308(a)(4)(ii)(A) Isolating health care clearinghouse function • 164.308(a)(4)(ii)(B) Access Authorization • 164.308(a)(4)(ii)(C) Access Establishment and Modification • 164.308(a)(5)(i) Log-in Monitoring • 164.308(a)(6)(ii) Response and Reporting • 164.312(a)(i) Access Control • 164.312(a)(2)(i) Unique User Identification • 164.312(a)(2)(ii) Emergency Access procedures • 164.312(a)(2)(iii) Automatic Logoff • 164.312(a)(ii)(iv) Encryption and Decryption • 164.312(b) Audit Controls • 164.312(c)(1) Data Integrity • 164.312(d) Person or Entity Authentication • 164.312(e)(i) Transmission Security • 164.312(e)(2)(i) Integrity Controls • 164.312(e)(2)(ii) Encryption

Table 4-1 HIPAA Safeguards Supported (continued)

Cisco Data Center Switches	• 164.308(a)(1)(i) Security Management Process • 164.308(a)(3)(i) Authorization/Supervision • 164.308(a)(4)(ii)(B) Access Authorization • 164.308(a)(5)(i) Log-in Monitoring • 164.308(a)(6)(ii) Response and Reporting • 164.312(a)(i) Access Control • 164.312(b) Audit Controls • 164.312(c)(1) Data Integrity • 164.312(e)(i) Transmission Security • 164.312(e)(2)(i) Integrity Controls • 164.312(e)(2)(ii) Encryption
Cisco DC IDSM	• 164.308(a)(1)(i) Security Management Process • 164.308(a)(3)(i) Authorization/Supervision • 164.308(a)(4)(ii)(B) Access Authorization • 164.308(a)(5)(ii)(B) Protection from Malicious Software • 164.308(a)(5)(i) Log-in Monitoring • 164.308(a)(6)(i) Security Incident Procedures • 164.308(a)(6)(ii) Response and Reporting • 164.312(a)(i) Access Control • 164.312(b) Audit Controls • 164.312(c)(1) Data Integrity • 164.312(e)(i) Transmission Security
Cisco MDS Switches	• 164.308(a)(1)(i) Security Management Process • 164.308(a)(4)(ii)(B) Access Authorization • 164.308(a)(5)(i) Log-in Monitoring • 164.308(a)(6)(i) Security Incident Procedures • 164.312(a)(i) Access Control • 164.312(a)(2)(iv) Encryption and Decryption • 164.312(b) Audit Controls • 164.312(c)(1) Data Integrity

Table 4-1 HIPAA Safeguards Supported (continued)

Cisco Nexus Switches	• 164.308(a)(1)(i) Security Management Process • 164.308(a)(3)(i) Authorization/Supervision • 164.308(a)(4)(ii)(A) Isolating health care clearinghouse function • 164.308(a)(4)(ii)(B) Access Authorization • 164.308(a)(5)(i) Log-in Monitoring • 164.308(a)(6)(i) Security Incident Procedures • 164.312(a)(i) Access Control • 164.312(b) Audit Controls • 164.312(c)(1) Data Integrity Security Management Process: • 164.308(a)(1)(i) Security Management Process Network Access Control: • 164.308(a)(4)(ii)(B) Access Authorization • 164.308(a)(4)(ii)(C) Access Est./ Modification Logging/Auditing/Monitoring: • 164.308(a)(5)(ii)(C) Log-in Monitoring • 164.308(a)(6)(ii) Response and Reporting • 164.312(b) Audit Controls

Table 4-1 HIPAA Safeguards Supported (continued)

Cisco Nexus VSG	• 164.308(a)(1)(i) Security Management Process • 164.308(a)(1)(ii)(D) Information System Activity Review • 164.308(a)(3)(i) Authorization/Supervision • 164.308(a)(4)(ii)(A) Isolating health care clearinghouse function • 164.308(a)(4)(ii)(B) Access Authorization • 164.308(a)(4)(ii)(C) Access Establishment and Modification • 164.308(a)(5)(i) Log-in Monitoring • 164.308(a)(6)(ii) Response and Reporting • 164.312(a)(i) Access Control • 164.312(a)(2)(i) Unique User Identification • 164.312(a)(2)(ii) Emergency Access procedures • 164.312(a)(2)(iii) Automatic Logoff • 164.312(a)(ii)(iv) Encryption and Decryption • 164.312(b) Audit Controls • 164.312(c)(1) Data Integrity • 164.312(d) Person or Entity Authentication • 164.312(e)(i) Transmission Security • 164.312(e)(2)(i) Integrity Controls • 164.312(e)(2)(ii) Encryption

Table 4-1 HIPAA Safeguards Supported (continued)

Cisco Wireless	• 164.308(a)(1)(i) Security Management Process • 164.308(a)(3)(i) Authorization/Supervision • 164.308(a)(4)(ii)(B) Access Authorization • 164.308(a)(5)(i) Log-in Monitoring • 164.308(a)(6)(i) Security Incident Procedures • 164.308(a)(6)(ii) Response and Reporting • 164.312(a)(i) Access Control • 164.312(a)(2)(i) Unique User Identification • 164.312(a)(2)(ii) Emergency Access procedures • 164.312(a)(2)(iii) Automatic Logoff • 164.312(a)(ii)(iv) Encryption and Decryption • 164.312(b) Audit Controls • 164.312(c)(1) Data Integrity • 164.312(d) Person or Entity Authentication • 164.312(e)(i) Transmission Security • 164.312(e)(2)(i) Integrity Controls • 164.312(e)(2)(ii) Encryption Security Management Process: • 164.308(a)(1)(i) Security Management Process Network Access Control: • 164.308(a)(4)(ii)(B) Access Authorization • 164.308(a)(4)(ii)(C) Access Est./ Modification Logging/Auditing/Monitoring: • 164.308(a)(5)(ii)(C) Log-in Monitoring • 164.308(a)(6)(ii) Response and Reporting • 164.312(b) Audit Controls

Table 4-1 HIPAA Safeguards Supported (continued)

EMC Clarion SAN	• 164.308(a)(1)(i) Security Management Process • 164.308(a)(3)(i) Authorization/Supervision • 164.308(a)(4)(ii)(B) Access Authorization • 164.308(a)(5)(i) Log-in Monitoring • 164.308(a)(6)(ii) Response and Reporting • 164.312(a)(2)(i) Unique User Identification • 164.312(b) Audit Controls • 164.312(c)(1) Data Integrity Security Management Process: • 164.308(a)(1)(i) Security Management Process Security Management Process: • 164.308(a)(1)(ii)(D) Information System Activity Review Information Access Management: • 164.308(a)(4)(ii)(B) Access Authorization Security Awareness and Training • 164.308(a)(5)(ii)(C) Log-in Monitoring Access Controls: • 164.312(a)(2) Access Controls Access Controls: • 164.312(a)(2)(i) Unique User Identification Audit Controls: • 164.312(b) Audit Controls Integrity: • 164.312(c)(1) Data Integrity Integrity: • 164.312(c)(2) Mechanism to Authenticate PHI Authentication: • 164.312(d) person or Entity Authentication

CHAPTER 5

Component Assessment

This chapter discusses the function of each component and how it helps to address HIPAA compliance requirements. Each component was assessed by Verizon Business, and the full reference architecture report is available in Appendix C, "Reference Architecture Assessment Report—Cisco Healthcare Solution."

This assessment took place at a specific point in time using currently available versions of products and software.

Component Section Overview

Each component section includes the following:

- Description
- Assessment summary
- Primary function
- Design considerations
- Assessment detail

Description

A high level overview of the products, features, and capabilities with relevance to compliance.

Assessment Summary

For each component, the Assessment Summary table lists each of the HIPAA safeguards that were addressed or failed.

Table 5-1 shows an example.

Table 5-1 PHI HIPAA Assessment Summary—Cisco ISR Router

Models Assessed	
CISCO891W version c890-universalk9-mz.151-3.T.bin	
CISCO1941W-A/K9 version c1900-universalk9-mz.SPA.151-3.T.bin	
CISCO2921/K9 version c2900-universalk9-mz.SPA.151-3.T.bin	
CISCO2951/K9 version c2951-universalk9-mz.SPA.151-3.T.bin	
CISCO3945-SPE150/K9 version c3900-universalk9-mz.SPA.151-3.T.bin	
HIPAA Safeguards Addressed	
Administrative	**Standards/Implementation Specifications**
164.308	(a)(1)(i) Security Management Process
	(a)(3)(i) Authorization/Supervision
	(a)(4)(i) Access Authorization
	(a)(5)(i) Log-in Monitoring
	(a)(6)(i) Response and Reporting
Technical	**Standards/Implementation Specifications**
164.312	(a)(1) Access Control
	(b) Audit Controls
	(e)(2)(ii) Encryption
HIPAA Standards Failed	
No HIPAA standards were failed.	
HIPAA Implementation Specifications Failed	
No HIPAA implementation specifications were failed.	

Primary Function

A HIPAA-relevant description of how this device is useful in an enterprise for addressing HIPAA compliance.

Design Considerations

This section provides compliance principles as well as best practices for each technology deployed within a clinic or hospital environment.

Assessment Details

A comprehensive list of the HIPAA safeguard citations addressed including sample device configurations.

Endpoints

The endpoints layer of the solution framework addresses the components such as voice, e-mail, and physical security.

Voice

Cisco Unified Communications Manager and IP Phones

The Cisco Unified Communication Manager is a suite of voice applications, signaling control, and utilities that provide IP communications capabilities using devices such as the IP phones. It is configured as an appliance that is easy to deploy, flexible to manage, and allows robust security.

Table 5-2 PHI HIPAA Assessment Summary—Cisco IP Voice Control

Models Assessed	
Cisco Unified Communication Manager 8.5.1	
HIPAA Safeguards Addressed	
Administrative	**Standards/Implementation Specifications**
164.308	(a)(1)(i) Security Management Process
	(a)(3)(i) Authorization/Supervision
	(a)(4)(i) Access Authorization
	(a)(6)(i) Response and Reporting
	(a)(6)(ii) Security Incident Procedures
Technical	**Standards/Implementation Specifications**
164.312	(a)(i) Access Control
	(b) Audit Controls
	(c)(1) Data Integrity
HIPAA Standards Failed	
No HIPAA standards were failed.	
HIPAA Implementation Specifications Failed	
No HIPAA implementation specifications were failed.	

Primary PHI Function

The primary function of the Cisco Unified Communications Manager in a healthcare network environment is to securely manage IP phones and communications flows, as well as securing publicly accessible network jacks in clinics and hospitals.

Design Considerations

The Cisco Unified Communication Manager is used to configure all of the communications infrastructure within the enterprise including ip phones, video endpoints, recording devices and conferencing bridges. Additionally it can also configure the flow of communications throughout the network.

The design features for improving security for the Cisco Unified Communications Manager appliance include:

- Deployment as a clustered redundancy model that includes a publisher server and several subscriber servers
- Downloading and installing security patches when vulnerabilities are announced by the Cisco Product Security Incident Response Team (PSIRT)
- Implementing Transport Layer Security (TLS) messaging for secure signaling and Secure RTP (SRTP) for encrypted media throughout the enterprise
- Enabling device authentication and communication encryption using X.509 certificates that are signed by the Certificate Authority Proxy Function (CAPF) feature on the server

Best practices for Cisco Unified Communications Manager phone security are as follows:

- Disable the gratuitous ARP setting on the Cisco Unified IP Phones.
- Disabling the web access setting prevents the phone from opening the HTTP port 80; this blocks access to the phone's internal web pages.
- Disabling the PC Voice VLAN access setting in the phone configuration window prevents the devices connected to the PC port from using the voice VLAN functionality.
- Disabling the Setting Access option in the phone configuration window prevents users from viewing and changing the phone options, including the Network Configuration options, directly on the phone.
- Cisco Unified IP Phones can be configured for authentication and encryption by installing a CTL file on the phones that includes security tokens, trusted server and firewall information, and CAPF.

For more information on securing Unified Communications, see the *Cisco Unified Communications System 8.x SRND* at the following URL:
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/8x/security.html

HIPAA Assessment Detail—HIPAA Safeguards Addressed

Here is a brief on communications from the HIPAA final rule:

Treatment sessions provided via video and audio conferencing software are not covered by the Security Rule. The HIPAA Final Rule specifically states "because 'paper-to-paper' faxes, person-to-person telephone calls, video teleconferencing, or messages left on voice-mail were not in electronic form before the transmission, those activities are not covered by this rule" (page 8342). If, however, the provider records the session and saves a copy, the saved version would be subject to Security Rule provisions for data at rest. Regardless, the treatment session and all related information and documentation from it are subject to the Privacy Rule provisions. To ensure the patient's privacy during treatment sessions, clinicians should consider the use of private networks or encrypted videoconferencing software.

The HIPAA definition of electronic media is as follows:

Subpart A – General Provisions

§160-103

Electronic Media means:

(1) Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card;

(2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

This solution validation did not include storage or recording of voice or video communications, therefore no implementation steps are shown on how to secure recorded ePHI.

All of the sample configurations shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
  - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
  - §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
  - §164.308(a)(6)(i) Security Incident Procedures. Implement policies and procedures to address security incidents.
  - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
  - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. Requirements addressed include: Auditing.
  - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
- Integrity—Protect electronic protected health information from improper alteration or destruction as required by HIPAA Technical safeguards.

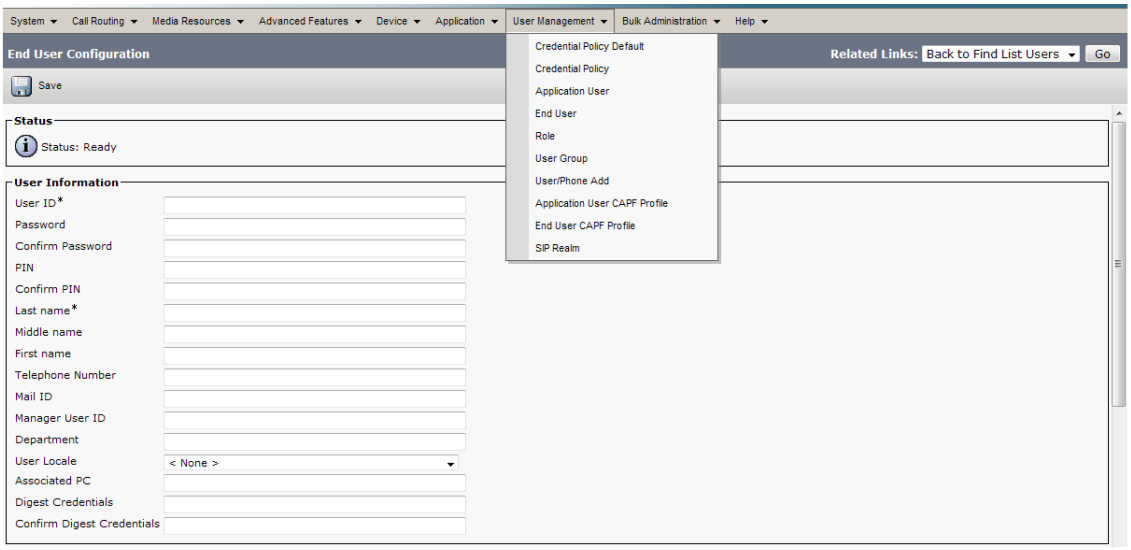
– §164.312(c)(1) Data Integrity. Implement policies and procedures to protect health information from improper alteration or destruction.

Sample Configuration

Cisco Unified Communication Manager is designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. They were met using the Cisco Unified Communication Manager's internal user database, because it has extensive features for administering users. Cisco Unified Communication Manager also supports linking to a centralized user database such as Active Directory using LDAP. Within Cisco Unified Communication Manager, individual user IDs are assigned and roles are based on group membership.

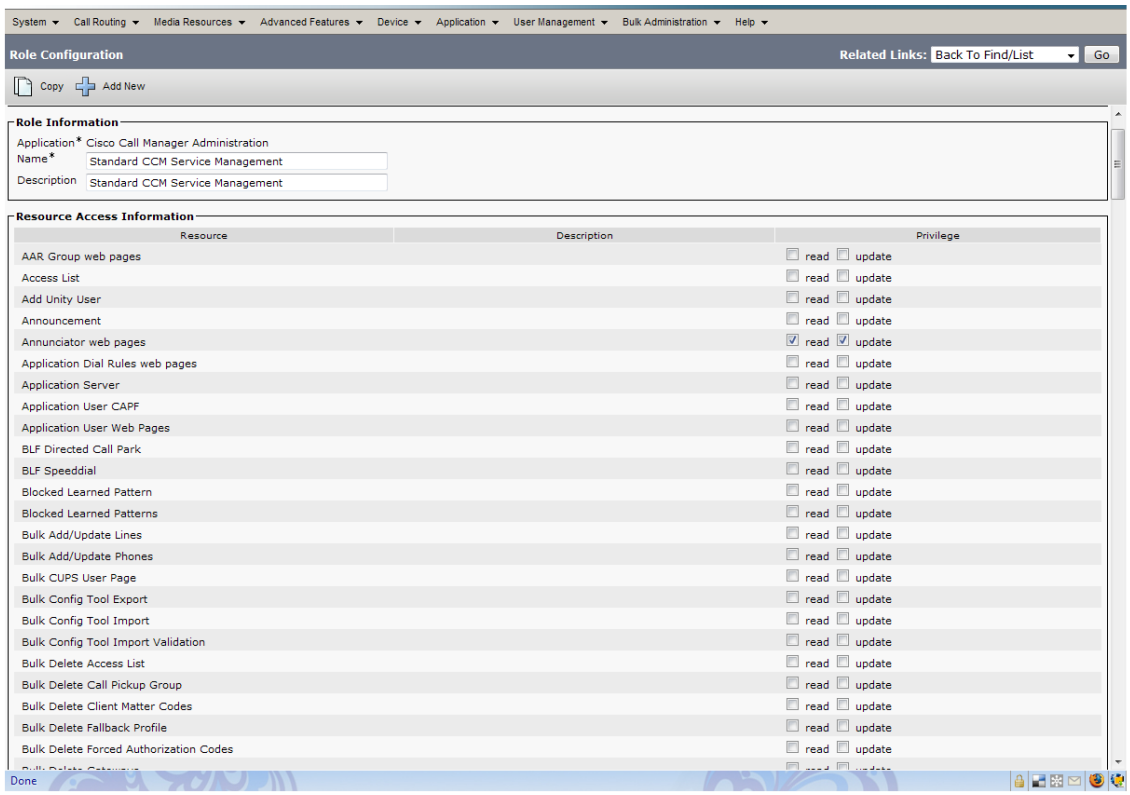
End users and administrators are added to the system by creating user IDs and passwords in the User Management section of the Cisco Unified Communication manager web interface, as shown in Figure 5-1.

Figure 5-1 End User Configuration



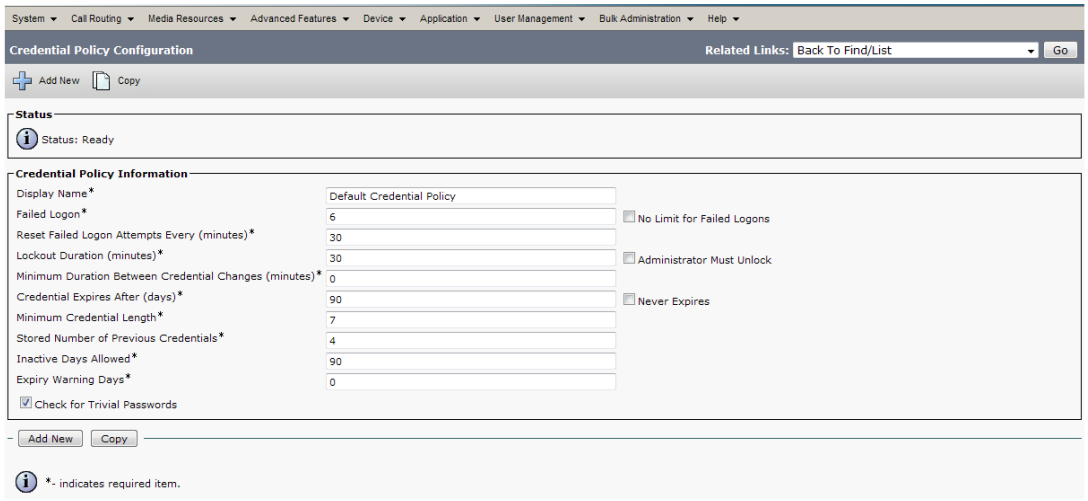
The role configuration menu in the Cisco Unified Communication Manager server allows specifying the assignment of privileges based on the role description. No systems access is permitted without an account. (See Figure 5-2.)

Figure 5-2 Role Configuration



Cisco Unified Communication Manager supports configuring a credential policy for user management and applying that policy to a designated group. Figure 5-3 shows a modified default credential policy.

Figure 5-3 User Credential Policy Configuration



The system provides trivial credential checks to disallow credentials that are easily hacked. You enable trivial credential checks by checking the Check for Trivial Passwords check box in the Credential Policy Configuration window.

Check for Trivial Passwords	Check this check box to require the system to disallow credential that are easily hacked, such as common words, repeated character patterns, and so on. The default setting checks the check box.

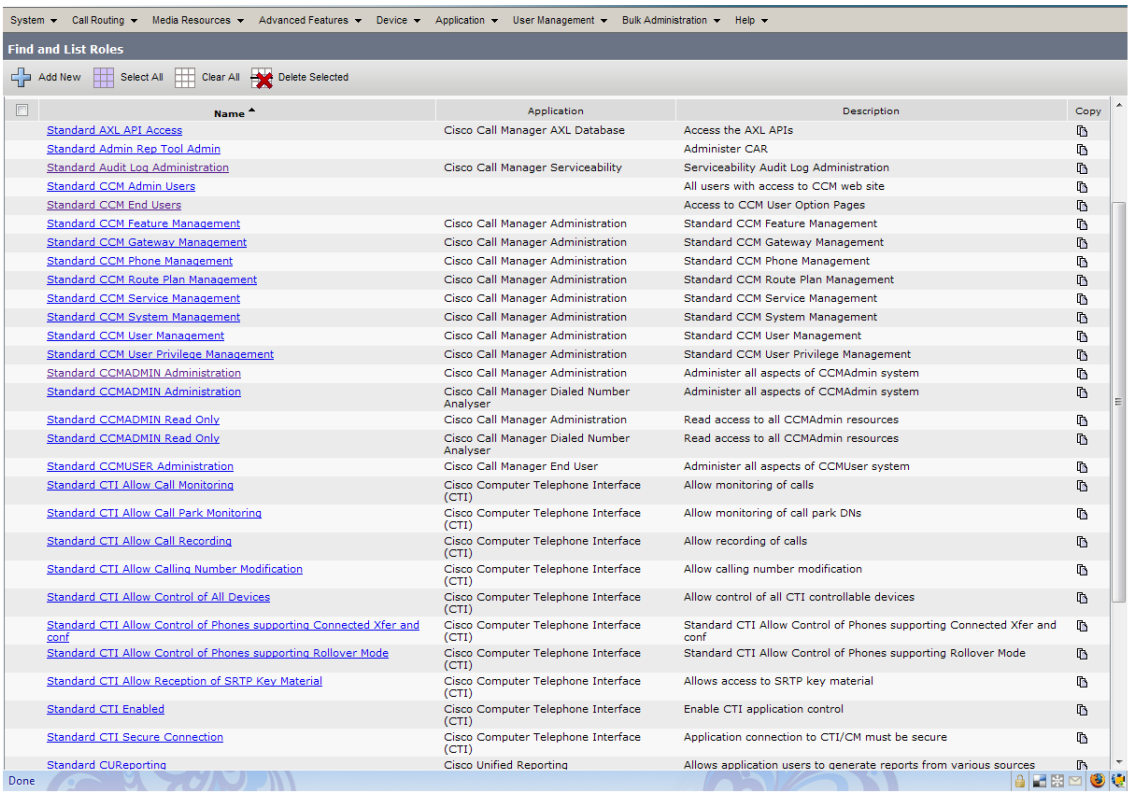
290984

Passwords can contain any alphanumeric ASCII character and all ASCII special characters. A non-trivial password meets the following criteria:

- Must contain three of the four allowable characteristics: uppercase character, lowercase character, number, and symbol.
- Must not use a character or number more than three times consecutively.
- Must not repeat or include the alias, username, or extension.
- Cannot consist of consecutive characters or numbers (for example, passwords such as 654321 or ABCDEFG)

The Cisco Unified Communication Manager uses various role definitions for permitting access to various application components on the server. (See Figure 5-4.)

Figure 5-4 Find and List Roles



290980

HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of automatic logoff options. Cisco Unified Communications Manager enforces this as part of the default system behavior. The system locks the user's session if the session has been idle for fifteen minutes, requiring the user to login again.

To address the Incident Response and Auditing HIPAA Safeguards identified above, Cisco Unified Communication Manager can be configured to send the logs to an external syslog server where it cannot be altered by the appliance users. Figure 5-5 and Figure 5-6 show the configurations necessary for log forwarding.

Figure 5-5 Enterprise Parameters Configuration

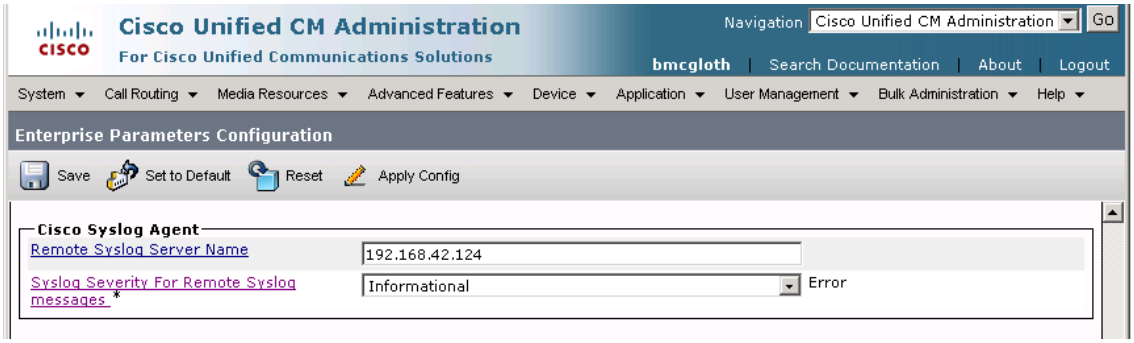
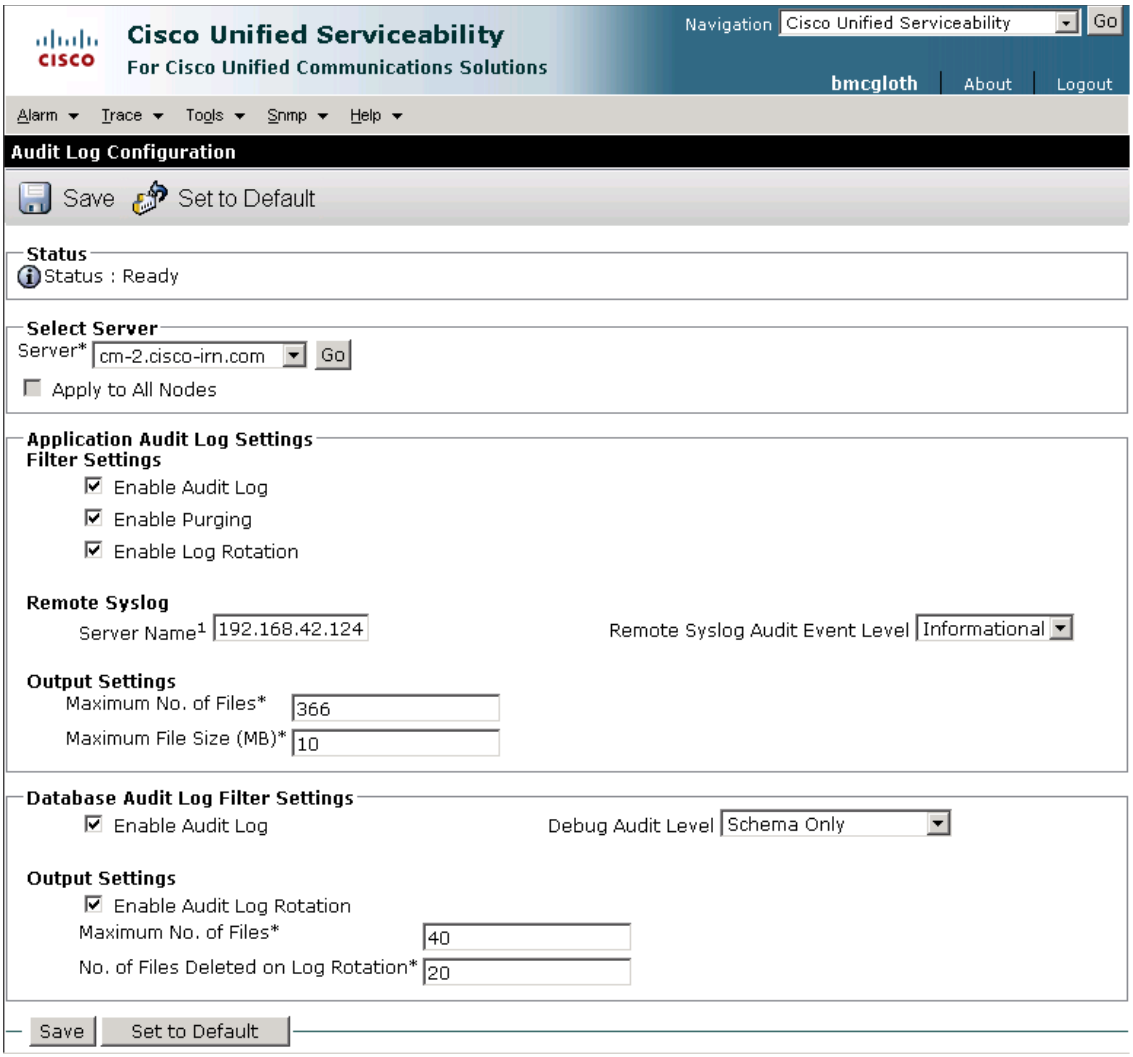


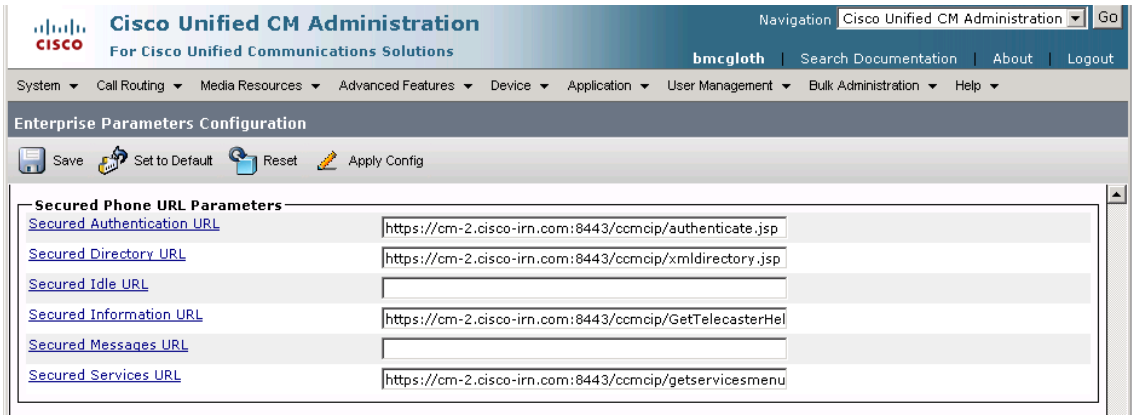
Figure 5-6 shows the necessary configuration under Cisco Unified Serviceability.

Figure 5-6 Audit Log Configuration



Within the Cisco Unified Communications Manager appliance operating system, root access to the OS is disabled and this prevents any unwanted services from being implemented. To secure authentication information and management of the server, addressing safeguard 164.308(a)(1)(i) Security Management, Telnet and HTTP access to the server for administration is disabled. The communication between phones and server over HTTP can be secured using SSL. (See Figure 5-7.)

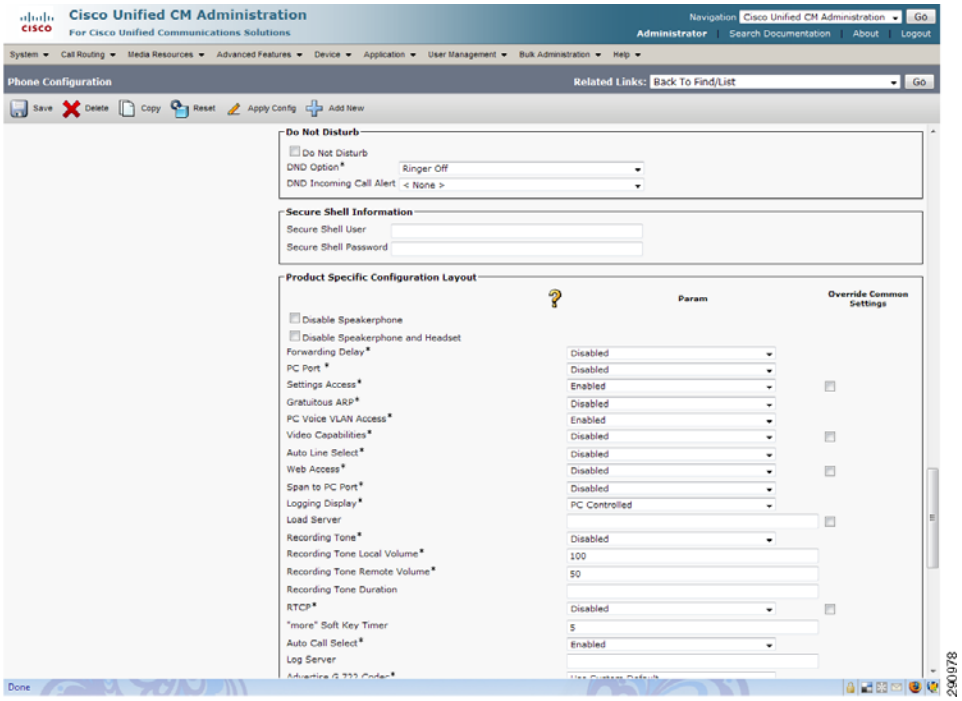
Figure 5-7 Enterprise Parameters Configuration



The Cisco Unified Communication Manager appliance does not allow changes to the operating system, or to the database or installation of unsupported hardware or of unsupported third-party software.

As a best practice, it is recommended to restrict physical and or logical access to publicly accessible network jacks. For example, areas accessible to visitors should not have network ports enabled unless network access is explicitly authorized. As Cisco IP phones include a pass-through port on them allowing a device to be connected to the network on which an IP phone resides, it is recommended to disable these ports or have them connect to a guest network segment when not intended for use on the ePHI network. Disabling the PC port can be accomplished in the phone configuration window for ports that are not in use, as shown in Figure 5-8.

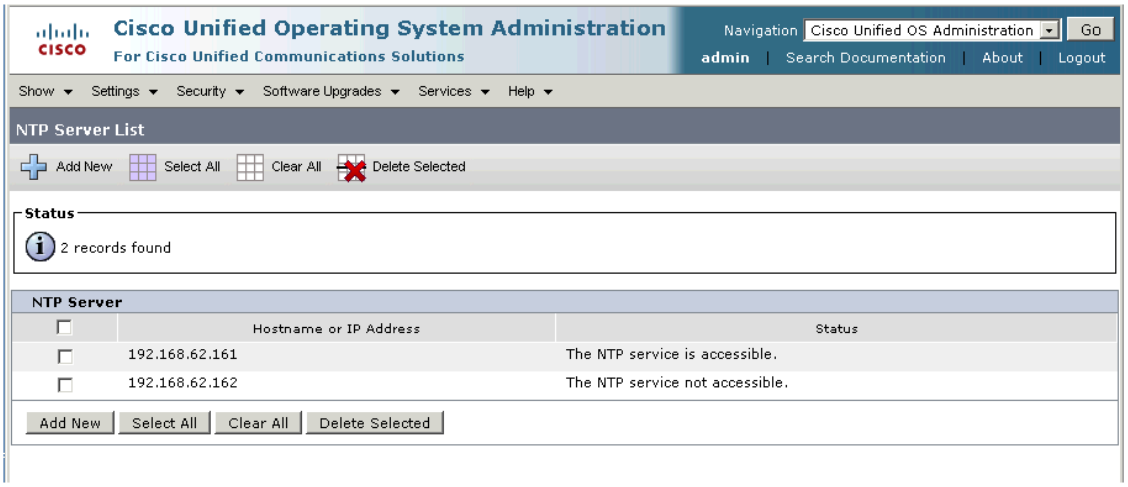
Figure 5-8 Phone Configuration



As a best practice, NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the

data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. Cisco Unified Communications Manager uses NTP by configuring the NTP server, as shown in Figure 5-9.

Figure 5-9 NTP Server List



Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Physical Security

Cisco Physical Security solutions provide broad capabilities in video surveillance, IP cameras, electronic access control, and groundbreaking technology that converges voice, data, and physical security in one modular platform. Cisco Physical Security solutions enable customers to use the IP network as an open platform to build more collaborative and integrated physical security systems while preserving their existing investments in analog-based technology. As customers converge physical security infrastructures and operations and begin using the IP network as the platform, they can gain significant value through rapid access to relevant information and interoperability between systems. This creates a higher level of situational awareness and allows intelligent decisions to be made more quickly.

Cisco Video Surveillance

Video surveillance technology provides security monitoring capabilities within a clinic, hospital, and data center environment. Video surveillance for loss prevention can now be extended into the area of protecting the ePHI data environment.

As the core component of Cisco's video surveillance software portfolio, the Cisco Video Surveillance Media Server offers the power and flexibility to meet a diverse range of video surveillance requirements. The media server:

- Uses IP technology to provide outstanding scalability in terms of sites, cameras, viewers, and storage
- Delivers low-latency, high-quality, event-tagged video
- Supports a broad range of cameras, codecs (such as JPEG, and MPEG-4, and H.264), viewing platforms, and network topologies
- Archives at various frame rates, durations, and locations

Quickly and effectively configure and manage video throughout your enterprise with the Cisco Video Surveillance Operations Manager (VSOM). Working in conjunction with the Cisco Video Surveillance Media Server and Cisco Video Surveillance Virtual Matrix, the Operations Manager meets the diverse needs of administrators, systems integrators, and operators by providing:

- A web-based toolkit for configuration, management, display, and control of video from a wide variety of both Cisco and third-party surveillance endpoints
- Management of a large number of Cisco Video Surveillance Media Servers, Virtual Matrixes, cameras, and users
- Flexible video recording options including motion-based, scheduled, and event-based
- Comprehensive control of users and user roles including scheduling of operator shifts, event filters, and user-specific video views
- Detailed activity reports and system audit

Table 5-3 PHI HIPAA Assessment Summary— Cisco Video Surveillance

Models Assessed	
Cisco Video Surveillance Manager version 6.3.1	
HIPAA Safeguards Addressed	
Administrative	**Standards/Implementation Specifications**
164.308	(a)(1)(i) Security Management Process
	(a)(3)(i) Authorization/Supervision
	(a)(4)(i) Access Authorization
	(a)(6)(i) Response and Reporting
	(a)(6)(ii) Security Incident Procedures
Physical	**Standards/Implementation Specifications**
164.310	(a)(1) Facility Access Controls
HIPAA Standards Failed	
No HIPAA standards were failed.	
HIPAA Implementation Specifications Failed	
No HIPAA implementation specifications were failed.	

Primary PHI Function

The primary function of video surveillance is to monitor physical access to sensitive areas within the ePHI data environment.

Design Considerations

- Ensure that cameras are positioned to monitor servers or systems within the ePHI data environment.
- Cameras should be appropriately positioned to identify personnel accessing these systems.
- Ensure adequate storage of video for three months or as specified by company policy.

For more information, see the Cisco IP Video Surveillance Guide at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/IPVS/IPVS_DG/IPVSchap4.html

A best practices guide is available for *Securing Cisco Video Surveillance Manage*r at the following URL: http://www.cisco.com/en/US/docs/security/physical_security/video_surveillance/network/design/bestprac.html#wp62691

HIPAA Assessment Detail—HIPAA Safeguards Addressed

All of the sample configurations of Cisco Video Surveillance shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict Access to ePHI Data as required by HIPAA Administrative and Technical Safeguards
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
  - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
  - §164.310(a)(1) Facility Access Control: Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.

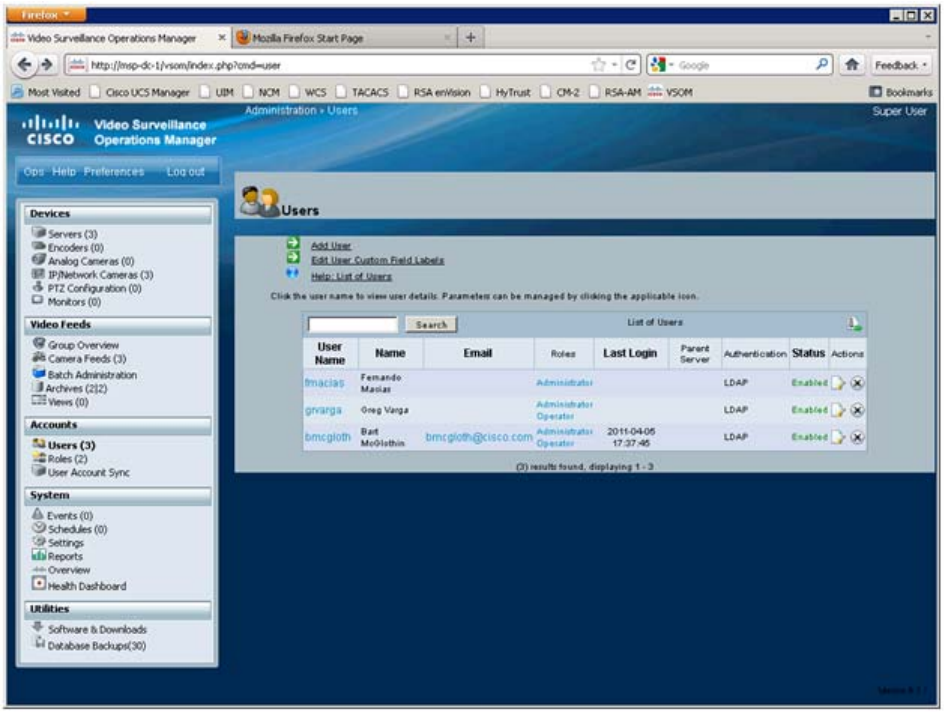
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.308(a)(6)(i) Response and Reporting. Implement policies and procedures to address security incidents. Requirements addressed include: Incident Response and Auditing.
  - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.

- Integrity—Protect electronic protected health information from improper alteration or destruction as required by HIPAA Technical safeguards.
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.

Cisco VSOM is designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership. The role configuration menu in the VSOM server allows specifying the assignment of privileges based on the role description. No systems access is permitted without an account.

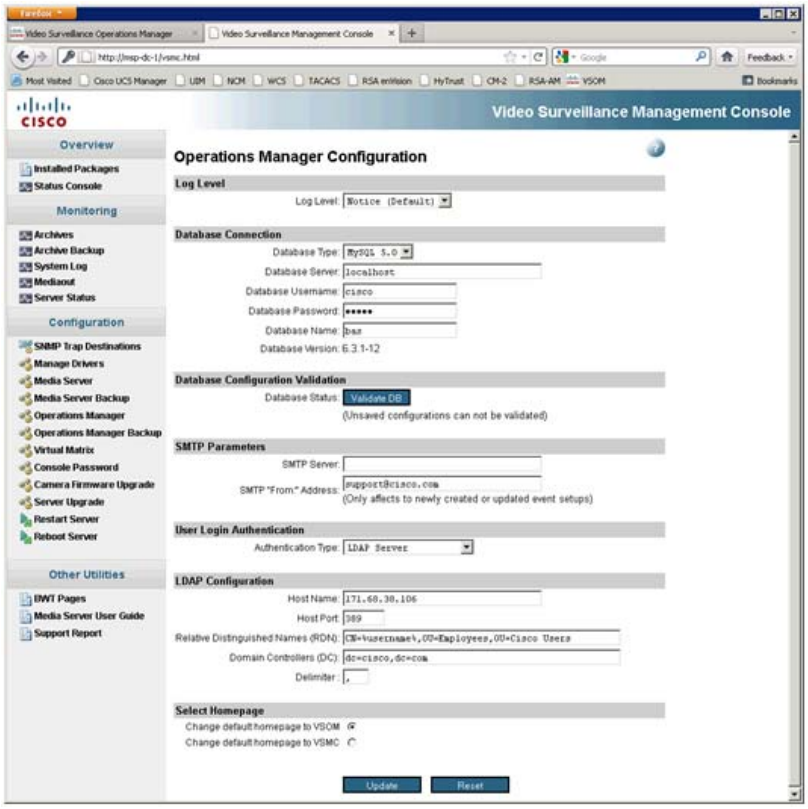
Individual users and roles are created locally and authentication directed to LDAP, as shown in Figure 5-10.

Figure 5-10 VSOM Users Authenticate to LDAP Service



Using the Video Surveillance Management Console, configure LDAP as specified in the installation guide. Figure 5-11 shows the LDAP configuration implemented for validation.

Figure 5-11 VSOM LDAP Configuration



HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of automatic logoff options. Cisco VSOM can be configured to enable session timeout and has a minimum session timeout of 30 minutes in the configuration for the version validated. To configure session timeouts navigate to Settings in the Administrator pages and select the Settings Tab.

To secure the authentication information and management of the server, addressing Safeguard 164.308(a)(1)(i) Security Management, the Cisco Video Surveillance Manager uses SSL for web-based administration and operator access, and uses SSH for remote terminal access. Use the Cisco Video Surveillance Operations Manager Secure Login feature, found within the Administrative Settings, to enable and force secure HTTPS application login. SSH access should be used to securely login to the VSM host.

To address the Incident Response and Auditing HIPAA Safeguards identified above, Cisco VSOM can be configured to send its log data to the RSA enVision log management platform. The following configuration script was implemented to send the local log files to the RSA enVision server to be secured and the integrity established:

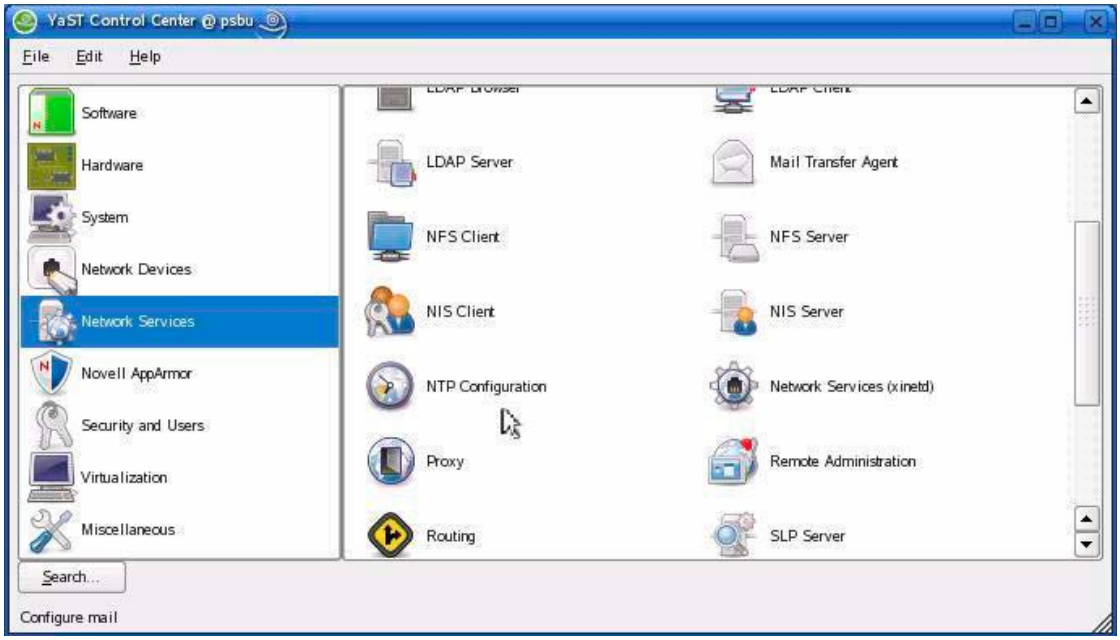
```
Directory:  /etc/cron.daily
Filename:  ftp-backup-files.cron

#!/bin/sh
FTP_USER=anonymous
FTP_PASS='vsom@cisco.com'
    localDIR="/usr/BWhttpd/bas/db/backups"
serverDIR="/vsom_backup/"
```

```
cd $localDIR
ftp -n -i 192.168.42.124    <<EOF
user $FTP_USER $FTP_PASS
binary
cd $serverDIR
mput VSOM_MSP-DC-1_backup_20$(date +%y%m%d)*.tar.gz
quit
EOF
exit 0
```

As a best practice, NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. Network Time Protocol (NTP) is supported and must be enabled within both the IP cameras and Video Surveillance Manager.

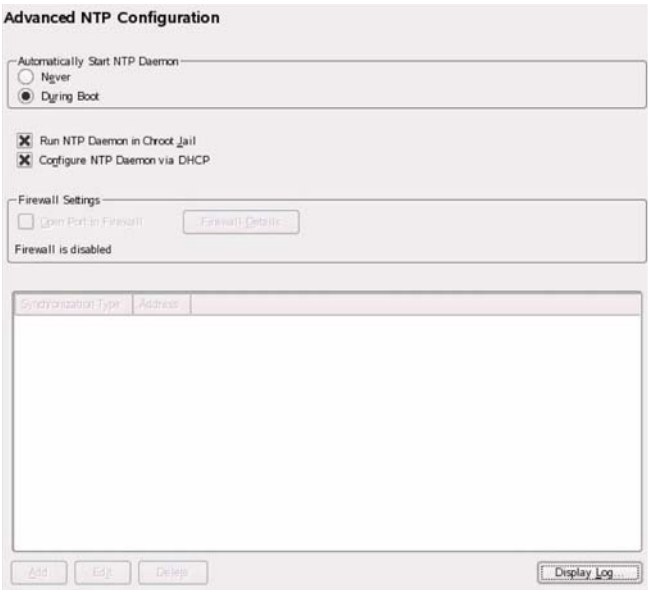
Step 1 In the YaST Control Center window, click **Network Services**, then click **NTP Configuration** in the right panel, as shown in Figure 5-12.

Figure 5-12 Accessing NTP Options



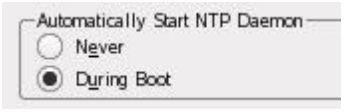
The Advanced NTP Configuration area appears, as shown in Figure 5-13.

Figure 5-13 Advanced NTP Configuration Area



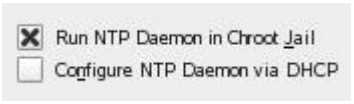
Step 2 Make sure that the During Boot radio button is selected, as shown in Figure 5-14.

Figure 5-14 Choosing the During Boot Radio Button



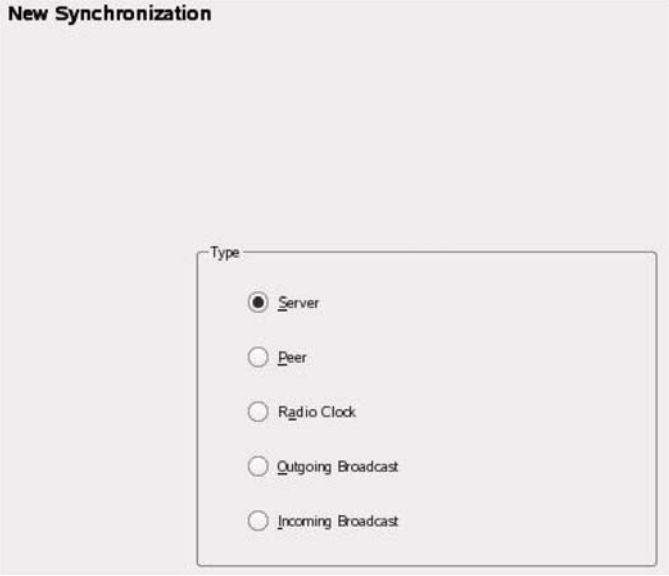
Step 3 Uncheck the **Configure NTP Daemon via DHCP** check box, as shown in Figure 5-15.

Figure 5-15 Unchecking the Configure NTP Daemon via DHCP Check Box



Step 4 Then click the **Add** button. The New Synchronization area appears, as shown in Figure 5-16.

Figure 5-16 New Synchronization Area



Step 5 In the New Synchronization area, make sure that the Server radio button is selected, and click **Next**.

The NTP Server panel appears, as shown in Figure 5-17.

Figure 5-17 NTP Server Area

Step 6 In the NTP Server area, take these actions:

a. In the Address field, enter the IP address or host name of your NTP server.

b. (Optional) Click **Test** to make sure that the Multi Services Platform can access the NTP server.

c. Check the **Use for Initial Synchronization** check box.

d. Click **OK**.

e. When complete, in the Advanced NTP Configuration screen, click **Finish**.

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

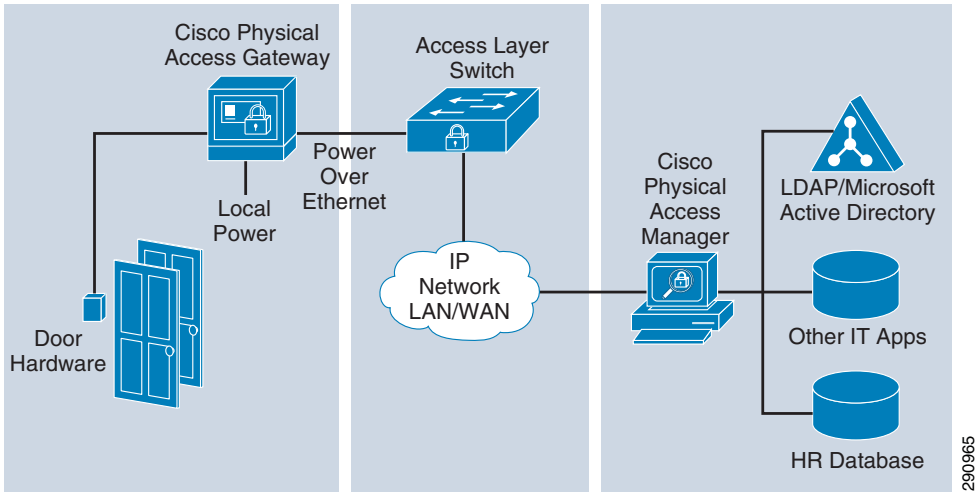
Cisco Physical Access Control

Cisco Physical Access Control allows organizations to secure their physical doors and locations. Cisco Physical Access Control addresses specific HIPAA safeguards by providing:

- Secure access to the server by supporting secure protocols such as HTTPS and also securing the accounts using strong passwords
- Role-based access to the system by making use of profiles that can restrict access to the modules, depending on the roles
- Automated backup of events to a centralized server
- Ability to archive audit reports on a centralized server

Cisco Physical Access Control is a comprehensive IP-based solution that uses the IP network as a platform for integrated security operations (see Figure 5-18). It works with existing card readers, locks, and biometric devices and is integrated with Cisco Video Surveillance Manager (VSM) and with Cisco IP Interoperability and Collaboration System (IPICS).

Figure 5-18 Scalable, Modular Architecture



Cisco Physical Access Control has two components:

- The hardware component, Cisco Physical Access Gateway, provides a modular and scalable platform to connect readers, inputs, and outputs to the system. The gateway scales from a single door to thousands of doors at a fixed cost per door.
- The software component, Cisco Physical Access Manager, manages the hardware, monitors activity, enrolls users, and integrates with IT applications and data stores.

Table 5-4 PHI HIPAA Assessment Summary—Cisco Physical Access Control

Models Assessed
Cisco Physical Access Manager version 1.2.0
HIPAA Safeguards Addressed

Table 5-4 PHI HIPAA Assessment Summary—Cisco Physical Access Control (continued)

Administrative	**Standards/Implementation Specifications**
164.308	(a)(1)(i) Security Management Process
	(a)(3)(i) Authorization/Supervision
	(a)(4)(i) Access Authorization
	(a)(6)(i) Response and Reporting
	(a)(6)(ii) Security Incident Procedures
Physical	**Standards/Implementation Specifications**
164.310	(a)(1) Facility Access Controls
HIPAA Standards Failed	
No HIPAA standards were failed.	
HIPAA Implementation Specifications Failed	
No HIPAA implementation specifications were failed.	

Primary PHI Function

The primary function of the CPAM appliance is to configure, manage, monitor, and report on the physical doors and door hardware, protecting sensitive areas within the healthcare ePHI data environment.

Design Considerations

Best practices are as follows:

- Use high availability for Cisco Physical Access Manager (PAM) servers.
- Map each branch location and identify the following:
  - Actual doors and modules
  - Door devices and module ports
- Use backup power supply for servers, modules, and devices.
- Cisco PAM was implemented following the Cisco Physical Access Manager Appliance User Guide, Release 1.2.0: http://www.cisco.com/en/US/docs/security/physical_security/access_control/cpam/1_2_0/english/user_guide/cpam_1_2_0.html

HIPAA Assessment Detail—HIPAA Safeguards Addressed

All of the sample configurations of the CPAM shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.

  - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
  - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
  - §164.310(a)(1) Facility Access Control: Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.308(a)(6)(i) Response and Reporting. Implement policies and procedures to address security incidents. Requirements addressed include: Incident Response and Auditing.
  - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
- Integrity—Protect electronic protected health information from improper alteration or destruction as required by HIPAA Technical safeguards.
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.

Sample Configuration

Cisco PAM is designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership.

Role-based access can be configured on Cisco PAM by making use of profiles. Profiles are pre-defined sets of access privileges that define the Cisco PAM modules and commands available to a user. For example, users that should have all privileges can be assigned to the Administrators profile.

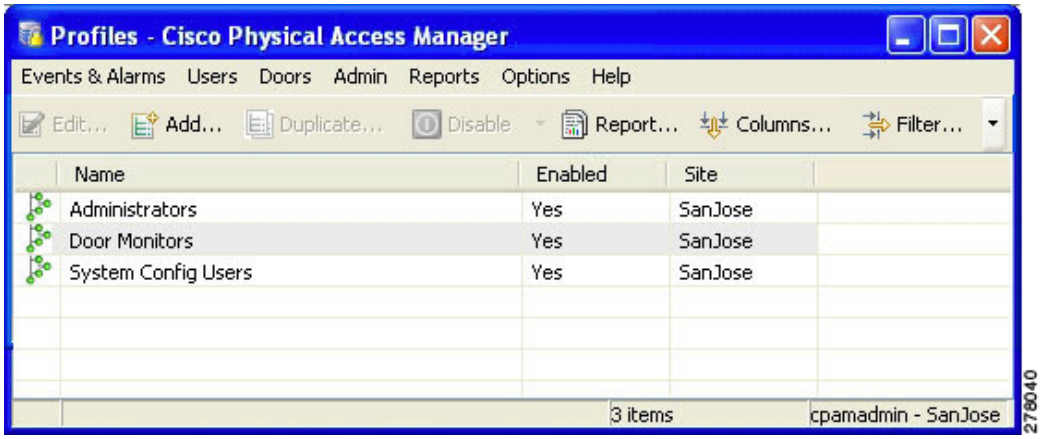
Note The Administrator profile is read-only and cannot be changed.

To create profiles, do the following:

Step 1 Select **Profiles** from the Users menu.

Step 2 To add a profile, choose Add.(See Figure 5-19.)

Figure 5-19 Profiles Module Main Window



Note To modify an existing profile, select the entry and choose **Edit**. To remove a profile, select the entry and choose **Delete**. The Administrator profile is read-only and cannot be changed.

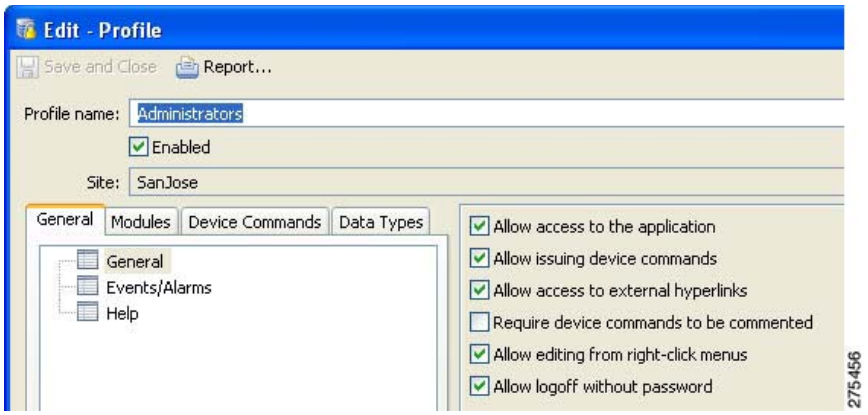
Step 3 Select a Profile template that most closely matches the desired level of user access, as shown in Figure 5-20:

- Default—A basic set of privileges is set.
- Most Restrictive—No privileges are set.
- Least Restrictive—All privileges are set.

Figure 5-20 Profile Templates

Step 4 Enter the basic profile settings, as shown in Figure 5-21.

Figure 5-21 Profile—General Tab



- Profile name—Enter a descriptive name for the profile.
- Enabled—Select the check box to enable the profile, or deselect the box to disable the profile.
- Partition—Select the partition from the drop-down menu.

Step 5 Click the **General** tab to define the basic profile properties. Click the checkbox next to each field to enable or disable the privilege, as described in Table 5-5.

Table 5-5 General Settings—Profile Module

Field	Description
General	
Allow access to the application	Allows access to the application.
Allow issuing device commands	Allows user to issue device commands directly to hardware.
Allow access to external hyperlinks	Allows access to external hyperlinks.
Require device commands to be commented	Requires the user to enter a comment with each device command issued in the system.
Allow editing from right-click menus	Allows access to the right-click the Edit menu.
Allow logoff without password	Allows user to logoff without a password.
Events/Alarms: Alarm Annotations (Ack., Clear, Comment)	
Allow annotations	Allows user to acknowledge, clear, and comment alarms. Click the **Filter** button to define the events that trigger the action.
Allow multiple annotations	Allows the user to acknowledge, clear, and comment multiple alarms at one time.
Allow clearing of unacknowledged alarms	Allows the user to clear unacknowledged alarms from active devices.
Allow clearing of active device alarms	Allows the user to clear alarms from active devices.
Events/Alarms—On new alarms	
Open Alarms Module	The **Alarms** module automatically opens with new system alarms. Click the **Filter** button to define the events that trigger the action.

Table 5-5 General Settings—Profile Module (continued)

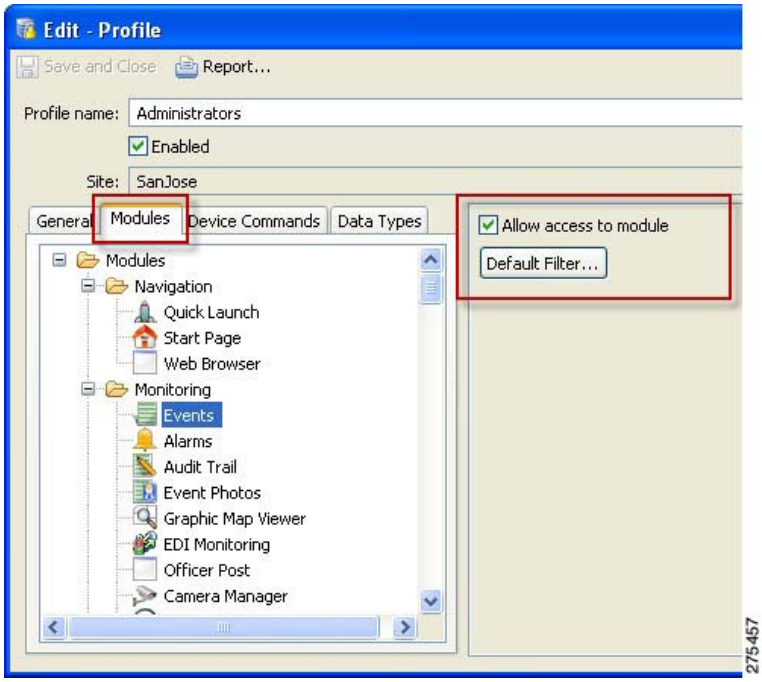
Open Manage Alarm window	The **Alarms** module automatically opens with new system alarms. Click the **Filter** button to define the events that trigger the action.
Open graphic map	The **Graphic Map** module automatically opens with new system alarms. Click the **Filter** button to define the events that trigger the action.
Show recorded video	Displays recorded video with new system alarms. Click the **Filter** button to define the events that trigger the action.
Show live video	Displays live video with new system alarms. Click the **Filter** button to define the events that trigger the action.
Help—Defines access to the various help systems	
Allow access to help documentation	Allows access to help documentation.
Enable context menu in help browser	Allows the user to view the help context menu.
Allow access to help PDF	Allows the user to access the help PDF. Adobe PDF viewer is required.

Step 6 Click the **Modules** tab to define the modules accessible to the profile, as shown in Figure 5-22.

a. Select a Cisco PAM module.

b. Select **Allow access to module** to enable access to the module.

Figure 5-22 Profile—Modules Tab



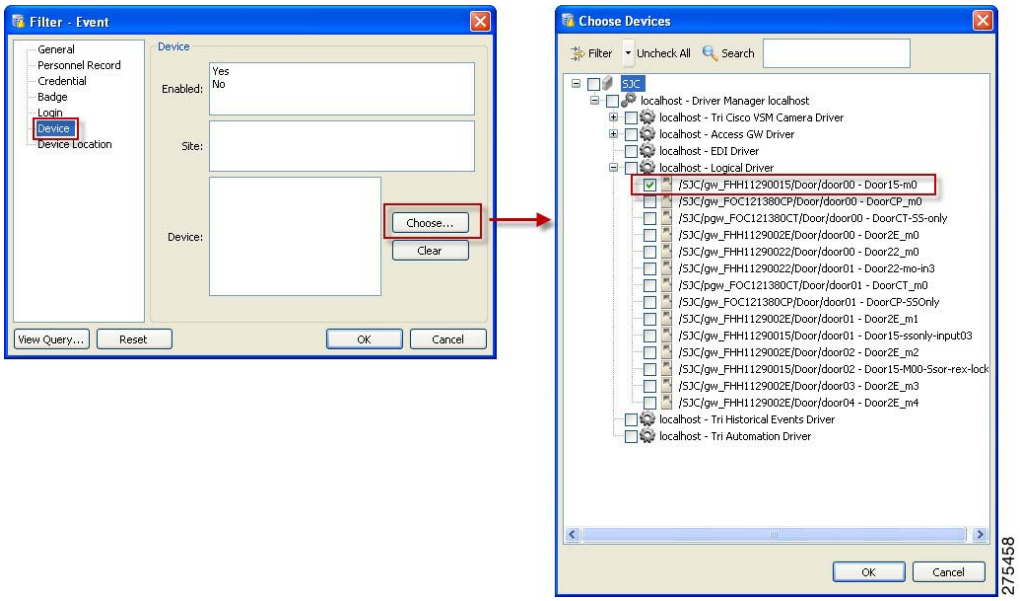
c. (Optional) Use the **Default Filter** with modules such as Event, Badge, and Personnel to define the filter applied when a user opens the module.

For example, to create a profile with access to the Events module that displays events for a specific door by default, complete the following sample steps:

1. Create a profile with access to the Events module, as described in the previous steps.
2. Click **Default Filter**, as shown in Figure 5-22.
3. Select the **Device** tab, as shown in Figure 5-23.
4. Click **Choose**.

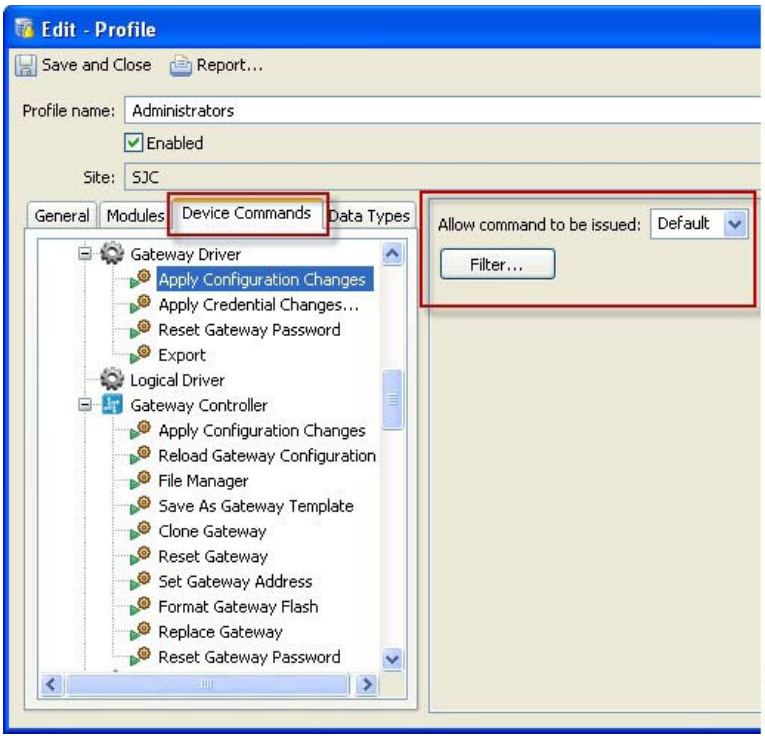
   In the Choose Devices window, expand the Logical Driver device tree and select a door (Figure 5-23).
5. Click **OK** to save the changes and close the windows.

Figure 5-23 Default Filter: Device Settings



Step 7 Click the **Device Commands** tab to define the hardware configuration commands available to the user (see Figure 5-24).

Figure 5-24 Profile—Device Commands Tab



a. Expand or collapse the list of commands for a device.

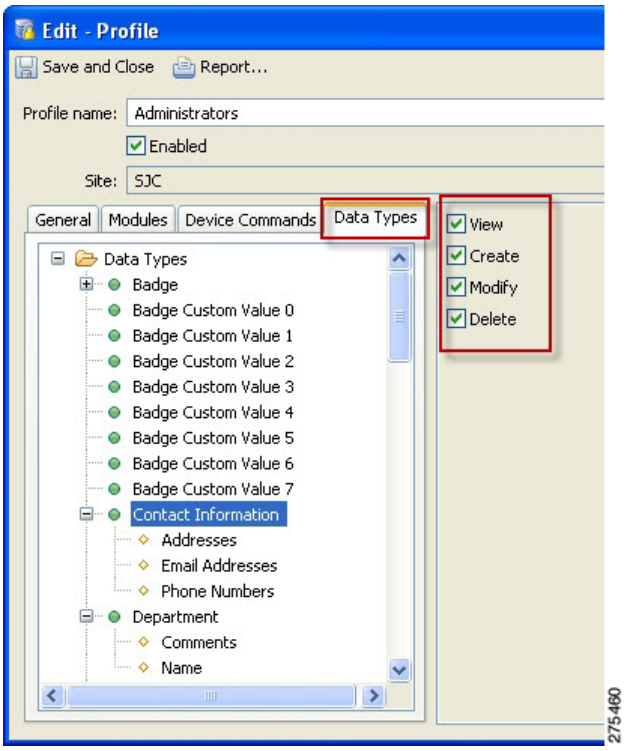
b. Highlight a command.

c. Select the following options:

- Allow command to be issued:
  - Default—If user has access to issue device commands, the command access is enabled by default.
  - No—Denies access to the command.
  - Yes—Allows access to the command.
- Filter—Apply a filter to limit the devices for the command.

Step 8 Click the **Data Types** tab to define the data available to the profile, as shown in Figure 5-25.

Figure 5-25 Profile—Data Types Tab



a. Select a module and the type of data in the list.

b. To restrict the data, click the check boxes for the properties listed in Table 5-6.

Table 5-6 Profile—Data Types

Field	Description
View	Allows the user to view the selected data type.
Create	Allows the user to add and create the selected data types.
Modify	Allows the user to modify existing data.
Delete	Allows the user to delete data.
Default Filter...	Allows the user to apply a default filter to limit objects from view.

Step 9 Click **Save and Close** to save the profile settings.

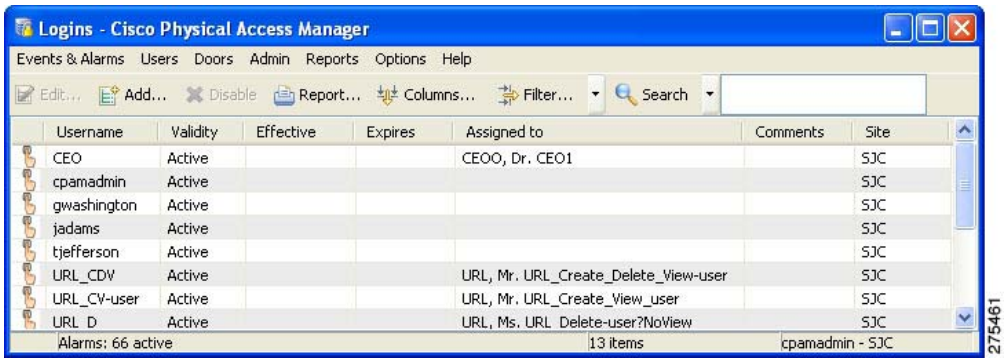
Step 10 Assign the profile to one or more Cisco PAM operators using the Logins module. (See the following section).

Creating User Login Accounts and Assigning Profiles

To give users access to Cisco PAM functionality, create a login account and assign one or more access profiles to the username.

Step 1 Select **Logins** from the Users menu. The main window (Figure 5-26) lists all the usernames in the system.

Figure 5-26 Logins Module Main Window



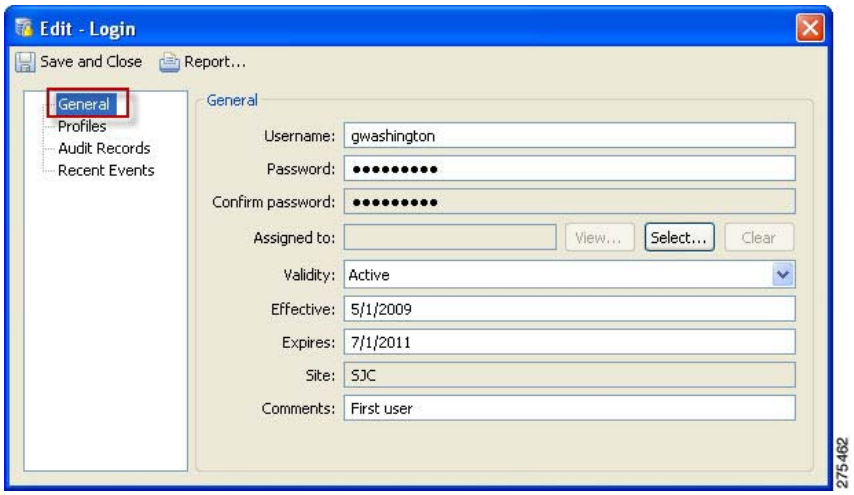
Step 2 To add a login, choose **Add**.

- To modify an existing login, select the entry and choose **Edit**.
- To remove a login, select the entry and choose **Delete**.

Note Most properties of the *cpamadmin* login are read-only.

Step 3 Complete fields in the General tab, as shown in Figure 5-27. Table 5-7 describes the field properties.

Figure 5-27 Logins Module—General Tab



Note The Username, Password, and Confirm password fields are required.

Table 5-7 General Tab Fields

Field	Description
Username	Required—The username of the login.
Password	Required—Password to access the system.
Confirm password	Required—The value must be entered exactly as it was in the Password field.

Table 5-7 General Tab Fields

Assigned to	The personnel record the login is assigned to. If the login is for an operator already entered in the Personnel module, click the **Select...** button. For more information on adding personnel to the system, see Chapter 8, "Configuring Personnel and Badges" of the CPAM User guide.
Validity	Active or Inactive—Only active accounts can access the system.
Effective	The beginning date the user can log in—If left blank, the user can log in immediately.
Expires	The day the login expires and access is denied—If left blank, access is allowed indefinitely.
Site	Read-only—A site is a single instance of a Cisco PAM database.
Comments	Comments or notes about the login.

Step 4 Assign access privileges for the login:

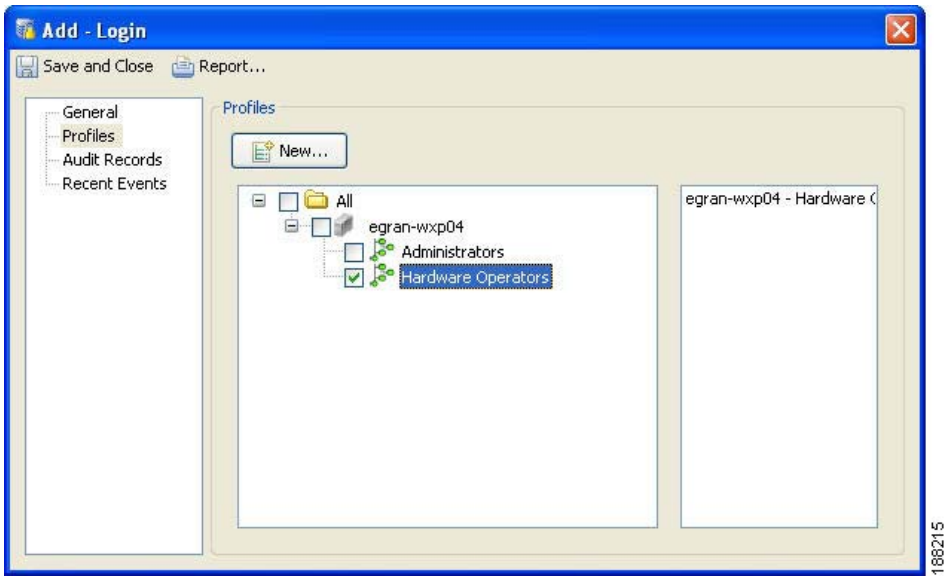
a. Select the **Profiles** tab, as shown in Figure 5-28.

b. Select the checkbox next to each profile to enable or disable access rights as defined by the access profile. For more information, see Defining User Profiles for Desktop Application Access.

c. Click **Save and Close** to save the changes and close the window.

Tip To create a new access profile, click the New button to open the Profiles module and refer to Defining User Profiles for Desktop Application Access.

Figure 5-28 Assigning One or More Profiles



Step 5 To verify the changes, log off and then log in with the new username and password. Verify that you can access the modules and functions specified by the assigned profiles.

Cisco PAM has a default policy of "Deny-all". If a specific badge has to get access to certain set of doors, an access policy must be created.

Cisco PAM supports authentication through LDAP. Because LDAP supports this feature, Cisco supports the methods listed above.

Configuring LDAP User Authentication on Cisco PAM

To authenticate users using a Lightweight Directory Access Protocol (LDAP) server, do the following:

1. Configure the LDAP Server
2. Create the LDAP User Account in Cisco PAM

Configure the LDAP Server

Enter the LDAP server settings to configure the LDAP server connection and user authentication, as described in the following steps.

Step 1 Select **System Configuration** from the Admin menu, and then select the **LDAP** tab.

Step 2 Enter the LDAP user authentication settings. The LDAP configuration depends on the authentication mode:

- User principal name (recommended method)—The user principal name is unique in the organization.
- sAMAccountName—The sAMAccount username is unique only in the search domain.

LDAP uses a principle to authenticate. The principle is formed from the username: prefix + username + suffix. The exact format of the principle varies based on the type of LDAP server, and the domain.

For OpenLDAP, the prefix should be: uid=
The suffix should be changed to reflect the actual domain.
So for my-domain.com, this would be:
,dc=my-domain, dc=com

For more information, see the following:

- LDAP Example: User Principal Name
- LDAP Example: sAMAccountName

Step 3 Enter the other LDAP server settings, as listed in Table 5-8.

Table 5-8 LDAP System Configuration Settings

Field	Description
Enable LDAP	Click the checkbox to enable or disable LDAP support.
LDAP server URL	URL of LDAP server, must begin with ldap:// Example: ldap://192.168.1.1:389 **Note** 389 is the port number.
Principle suffix	Appended to the username for authentication. See above.
Principle prefix	Prepended to the username for authentication. See above.

Table 5-8 LDAP System Configuration Settings (continued)

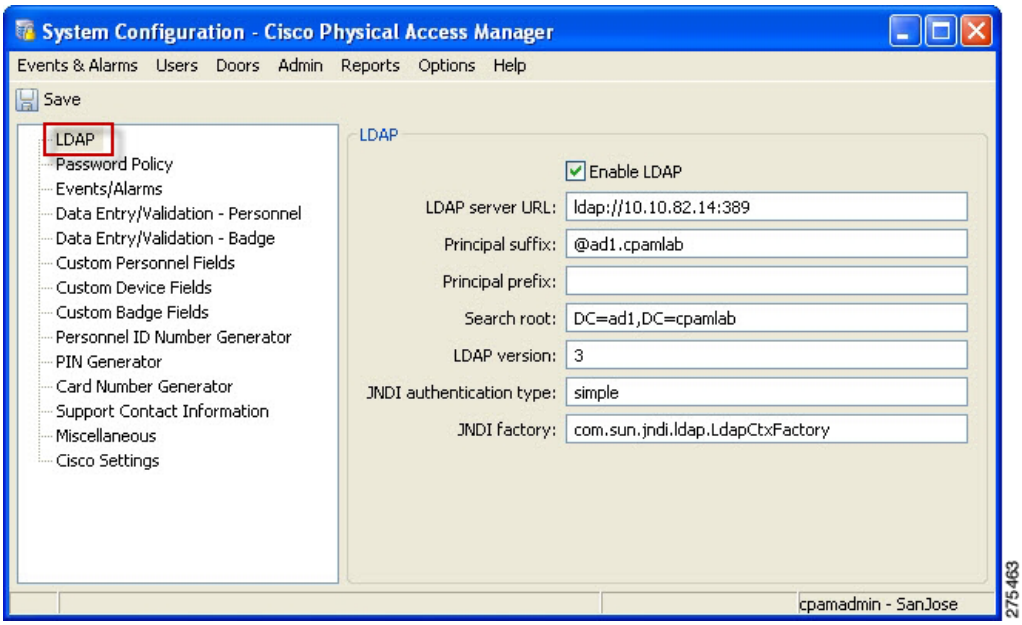
Search root	LDAP search root. The search root is the node in the LDAP tree, the subtree under which the user account should be found. • For Active Directory, the dc components should be changed to match the full domain name managed by the directory. The following example is for my-domain.com: cn=Users, dc=my-domain, dc=com. • For OpenLDAP, the 2 dc components should be changed to match the full domain name managed by the directory. The following example is for my-domain.com:dc=my-domain,dc=com.
LDAP version	An advanced setting that generally should be left unchanged.
JNDI authentication type	An advanced setting that generally should be left unchanged as simple.
JNDI factory	An advanced setting that generally should be left unchanged as com.sun.jndi.ldap.LdapCtxFactory

Step 4 Log out and log back in to the Cisco PAM application to enable the changes (select **Logout** from the Options menu).

LDAP Example—User Principal Name

In the example shown in Figure 5-29, the user principal name is *cpsm.user@ad1.cpamlab*. The Cisco PAM user login must be the same (*cpsm.user*).

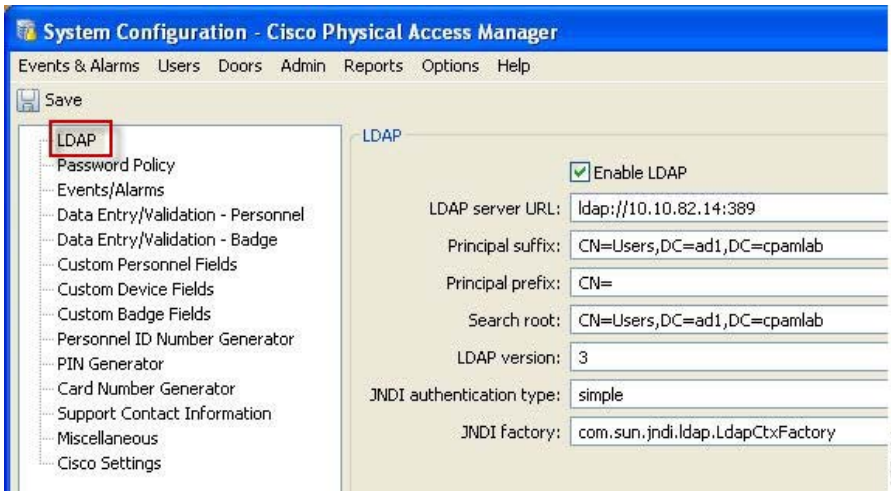
Figure 5-29 User Principal LDAP Configuration Example



LDAP Example—sAMAccountName

In the example shown in Figure 5-30, the user login is the same as the samaccount name (*cpsmuser*).

Figure 5-30 sAMAccountName—LDAP Configuration Example

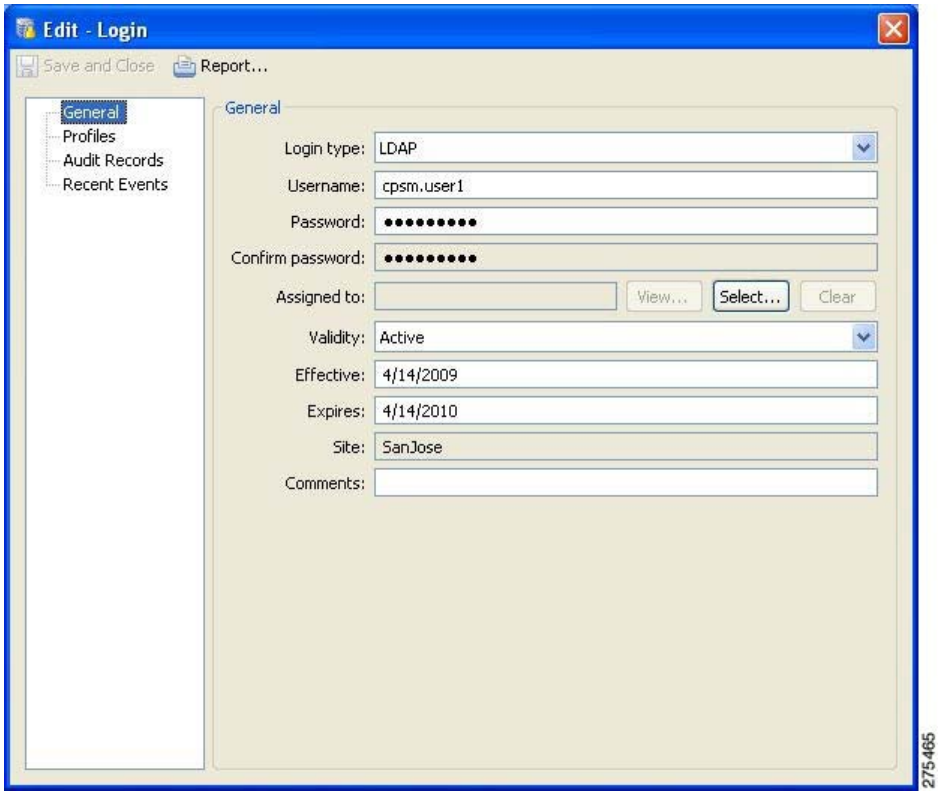


Creating the LDAP User Account in Cisco PAM

Create the user account to be authenticated using an LDAP server with the following steps.

Step 1 Select **Logins** from the Users menu. (See Figure 5-31.)

Figure 5-31 Login Window: LDAP Login Type



Step 2 Click **Add**, or select an existing login and click **Edit**.

Step 3 Select the Login type **LDAP**. The Login type field appears only if LDAP was enabled and the Cisco PAM application was restarted (see Configure the LDAP Server).

Step 4 Enter the username, password, and other settings for the LDAP login. See Creating User Login Accounts and Assigning Profiles.

Note Although a password must be entered for all user Login records, it is not used for LDAP authentication. LDAP servers use the password entered when the user logs in to Cisco PAM.

Step 5 Click **Profiles** and select the user's Cisco PAM profiles. See Defining User Profiles for Desktop Application Access for more information.

Note Cisco PAM does not synchronize the LDAP profiles.

Step 6 Click **Save and Close**.

To secure authentication information and management of the server, addressing Safeguard 164.308(a)(1)(i) Security Management, SSL is enabled by default on the Cisco PAM appliance. All the communication between the Cisco PAM client and the gateway is encrypted using the 128-bit AES encryption. Console access to Cisco PAM is through SSH. The Cisco PAM appliance should also be configured to disable unsecure protocols. To disable unsecure protocols, you must edit one of the configuration files on the Cisco PAM appliance. The step-by-step instructions are as follows:

1. SSH into the Cisco PAM server
2. sudo su
3. Enter the cpamadmin password
4. Stop the service: /etc/init.d/cpamadmin stop
5. Comment out a configuration from the file /opt/cisco/cpam/apache-tomcat/conf/server.xml.

   Remove or comment the snippet below.

```
<Connector executor="tomcatThreadPool"
port="8080" protocol="HTTP/1.1"
connectionTimeout="20000"
redirectPort="8443" />
```

6. Re-start the service: /etc/init.d/cpamadmin start

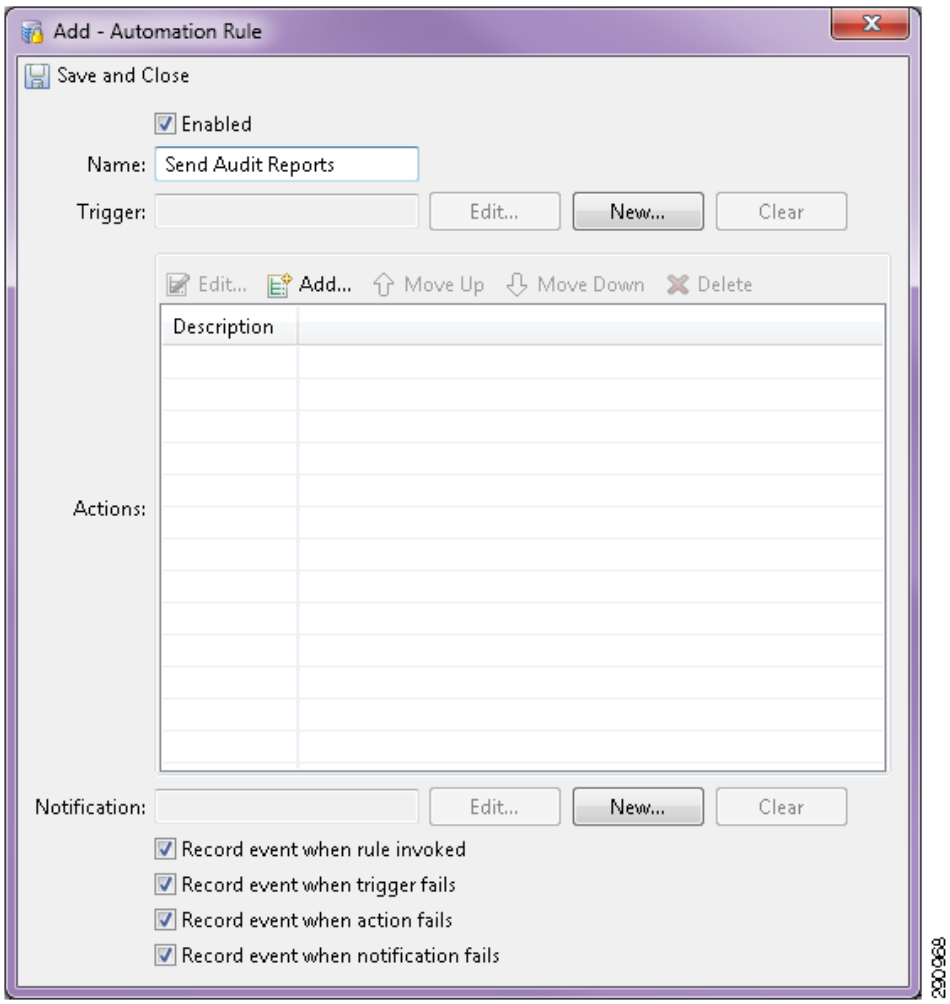
When you try to launch the web UI using HTTP, you see “Page cannot be displayed”.

To address the Incident Response and Auditing HIPAA Safeguards identified above, Cisco PAM allows for the creation of global I/O rules to trigger sending audit reports to a centralized server. Following are the instructions to create a global I/O with audit reports.

Step 1 In the Cisco PAM client, click **Events & Alarms -> Global I/O > Add**.

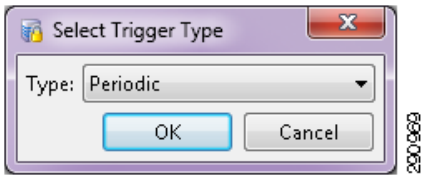
Step 2 Enter a name and click **New** in the Trigger field. (See Figure 5-32.)

Figure 5-32 Creating a Global I/O with Audit Reports



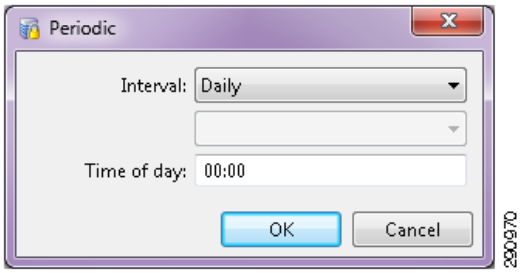
Step 3 Select **Periodic** and click **OK**. (See Figure 5-33.)

Figure 5-33 Selecting Periodic



Step 4 Choose the Interval and enter the Time of Day. Click **OK**. (See Figure 5-34.)

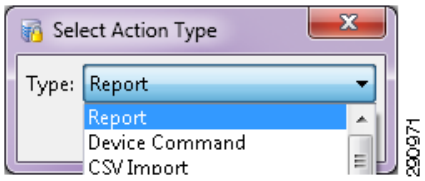
Figure 5-34 Selecting Interval and Time of Day



Step 5 Under Actions, Click **Add…**

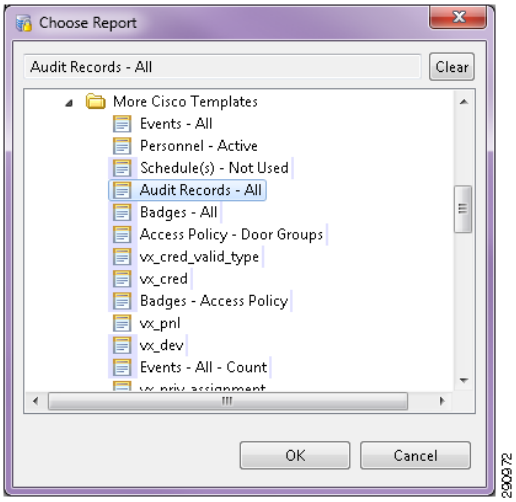
Step 6 Select **Report.** (See Figure 5-35.)

Figure 5-35 Selecting Action Type



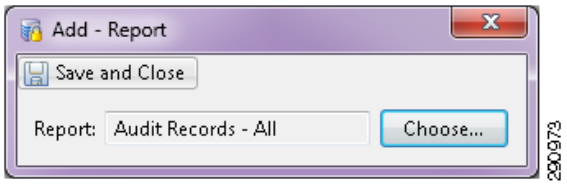
Step 7 Choose **Audit Records–All** and click **OK**. (See Figure 5-36.)

Figure 5-36 Audit Records–All



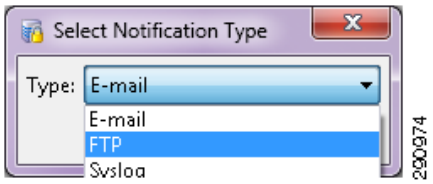
Step 8 Click **Save and Close**. (See Figure 5-37.)

Figure 5-37 Save and Close



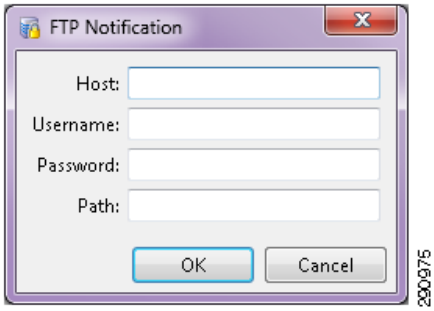
Step 9 Under Notification section of the Global I/O, click **New** and Choose **FTP**. Click **OK**. (See Figure 5-38.)

Figure 5-38 Select Notification Type



Step 10 Enter the FTP Host, Username, Password, and Path. Click **OK**. (See Figure 5-39.)

Figure 5-39 FTP Notification



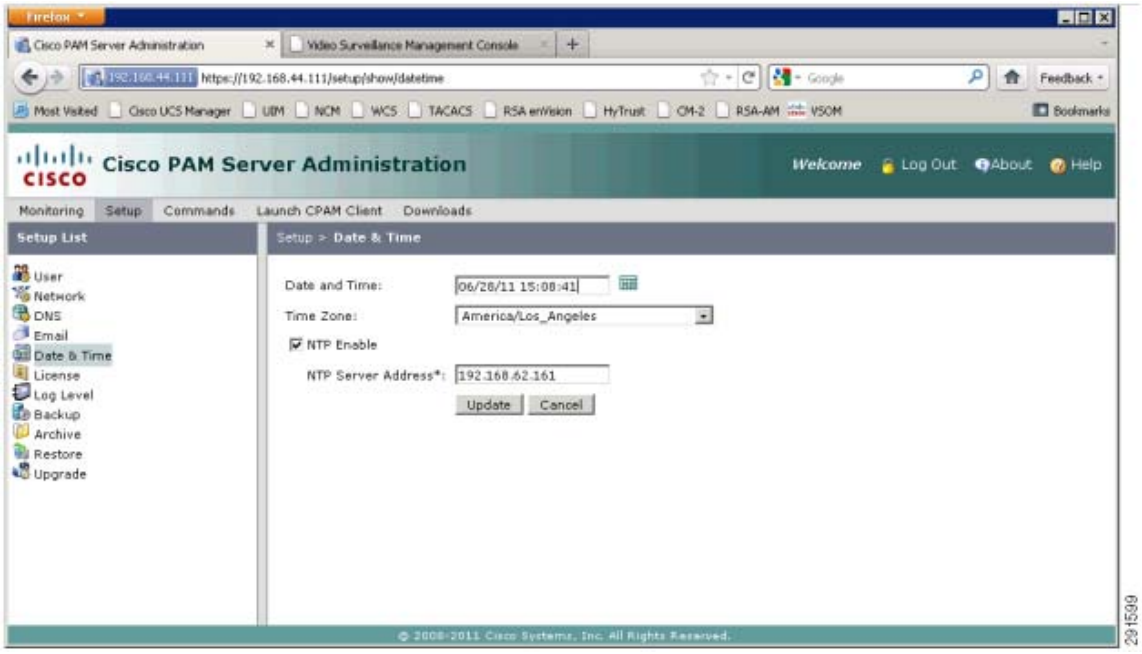
Step 11 Click **Save and Close**. You should see a new entry created. You can create similar global I/O rules for every hour.

The audit report is read into RSA enVision server, which then maintains and protects the integrity of the file.

HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of automatic logoff options. Cisco PAM has a hard-coded session timeout of 30 minutes in the configuration for the version validated.

As a best practice, NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. All the events in the Access Control system have a time stamp associated to them. Cisco PAM and the gateway are configured to use NTP, as shown in Figure 5-40.

Figure 5-40 Cisco PAM NTP Configuration



HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Cisco Unified Computing System

The Cisco Unified Computing System (UCS) is designed to securely deploy sensitive and compliance-related applications. Provisioning options, including virtualization technology, allow the mixing of sensitive and non-sensitive applications without compromising scope boundaries.

Improve IT responsiveness to rapidly changing business demands with this next-generation data center platform. Cisco UCS accelerates the delivery of new services simply, reliably, and securely through end-to-end provisioning and migration support.

Benefits include the following:

- Streamlines data center resources to reduce total cost of ownership
- Scales service delivery to increase business agility
- Radically reduces the number of devices requiring setup, management, power, cooling, and cabling

Table 5-9 PHI HIPAA Assessment Summary—Cisco UCS

Models Assessed
Cisco UCS Manager version 1.3(1p)
HIPAA Safeguards Addressed

Table 5-9 PHI HIPAA Assessment Summary—Cisco UCS (continued)

Administrative	Standards/Implementation Specifications
164.308	(a)(1)(i) Security Management Process
	(a)(3)(ii)(A) Authorization/Supervision
	(a)(4)(ii)(A) Isolating Clearing House Functions
	(a)(4)(ii)(B) Access Authorization
	(a)(5)(ii)(C) Log-in Monitoring
	(a)(6)(ii) Response and Reporting
Technical	**Standards/Implementation Specifications**
164.312	(a)(i) Access Control
	(b) Audit Controls
	(c)(1) Data Integrity
HIPAA Standards Failed	
No HIPAA standards were failed.	
HIPAA Implementation Specifications Failed	
No HIPAA implementation specifications were failed.	

Primary PHI Function

The primary function of Cisco UCS is to securely host one primary compliance-related function per physical or virtual server.

It provides segmentation of sensitive applications from out-of-scope applications via physical and virtualization technology. Cisco UCS extends Layer 3 boundaries to virtual network and storage adapters within the chassis. Using VLANs and VSANs, Cisco UCS allows an organization to separate its ePHI systems (in-scope) from other non-sensitive data (out-of-scope).

Design Considerations

- Cisco UCS allows for the provisioning of individual servers on blades. Each blade can host a native operating system such as Windows 2008 server, or a virtualization hypervisor system such as VMware ESX/ESXi. These provisioning options represent a primary function for the server blade. In the lab validation, VMware ESX was installed on each of the Cisco UCS blades, and several VM hosts were then configured, each with one primary function. Each server blade is provisioned via a profile. Profiles can be created locally in Cisco UCS Manager or centrally using the Vblock provisioning utility, Unified Infrastructure Manager (UIM), which provides simplified Vblock management by combining provisioning with configuration, change, and compliance management.
- EMC SAN is a primary component of the VCE architecture for Vblock Infrastructure Platforms. Vblock 1 is designed for medium to high numbers of virtual machines, and is ideally suited to a broad range of usage scenarios, including shared services, e-mail, file and print, virtual desktops, and collaboration.
- Cisco UCS allows for the provisioning of individual servers on blades. Each blade can host a native operating system such as Windows 2008 server, or a virtualization hypervisor system such as VMware ESX/ESXi.

- Each Cisco UCS server blade is provisioned via a profile. Profiles can be created locally in Cisco UCS Manager or centrally using the Vblock provisioning utility, EMC Unified Infrastructure Manager (UIM), which provides simplified Vblock management by combining provisioning with configuration, change, and compliance management.
- The hypervisor of an individual blade is considered insecure for segmenting scopes of compliance. Therefore, when putting non-sensitive VM servers with sensitive VM servers on the same physical blade, the non-sensitive would be included in the scope of the audit.
- The UCS system securely segments network and storage to each blade, which allows mixing of sensitive and non-sensitive applications across different physical blades of the chassis.
- Cisco UCS does not feature an explicit session timeout. Administration time limits would need to be enabled systemically through active directory policy to the admin workstation desktops, locking them when there is no activity.

  Cisco UCS was implemented using the Cisco UCS installation guides: http://www.cisco.com/en/US/products/ps10276/prod_installation_guides_list.html

HIPAA Assessment Detail—HIPAA Safeguards Addressed

All of the sample configurations of the Cisco UCS shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
  - §164.308(a)(4)(ii)(A) Isolating healthcare clearinghouse function. If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. Requirements addressed include: Access Control, Integrity, Incident Response and Auditing.
  - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
  - §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4). Requirements addressed include: Access Control and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. Requirements addressed include: Auditing.

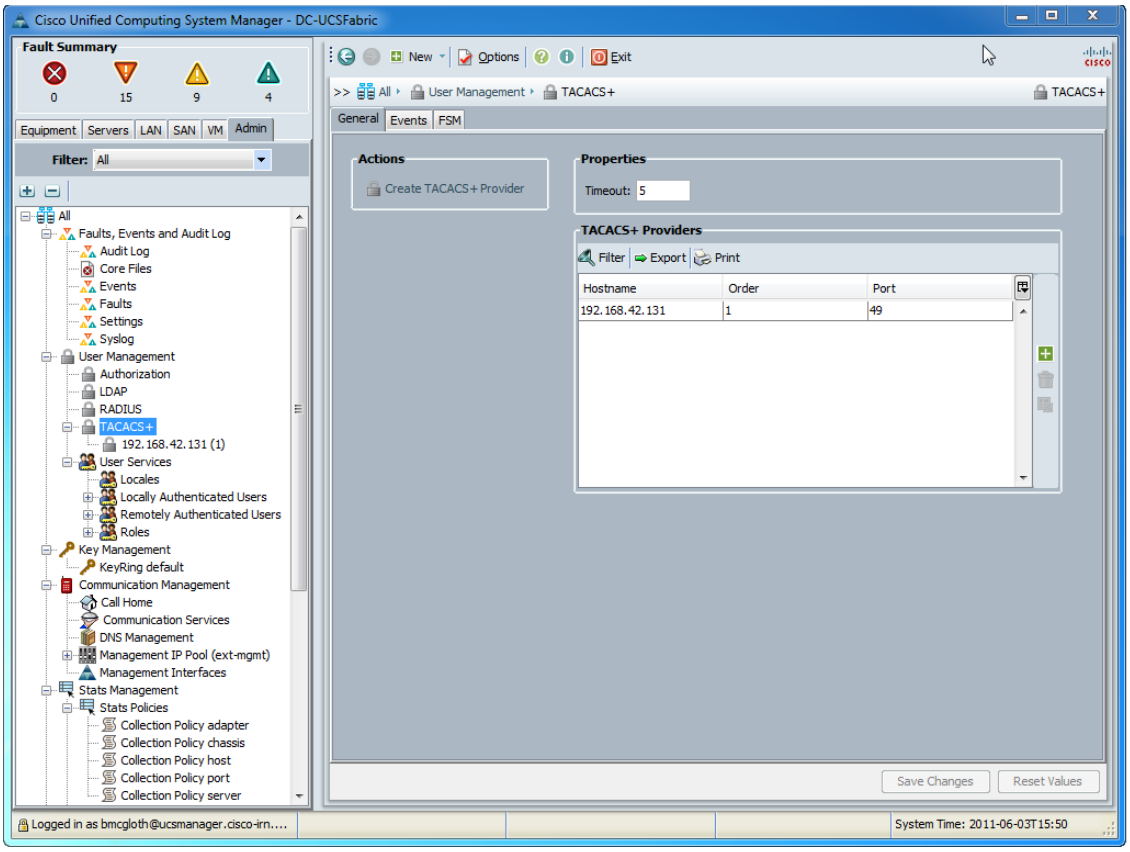
  - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
  - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
  - §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4). Requirements addressed include: Access Control and Auditing.
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.308(a)(6)(i) Response and Reporting. Implement policies and procedures to address security incidents. Requirements addressed include: Incident Response and Auditing.
  - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
- Integrity—Protect electronic protected health information from improper alteration or destruction as required by HIPAA Technical safeguards.
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.312(c)(1) Data Integrity. Implement policies and procedures to protect health information from improper alteration or destruction.

Sample Configuration

Cisco UCS servers are able to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership. Cisco UCS includes extensive controls for defining user privileges and by default denies access to all individuals without a system user ID.

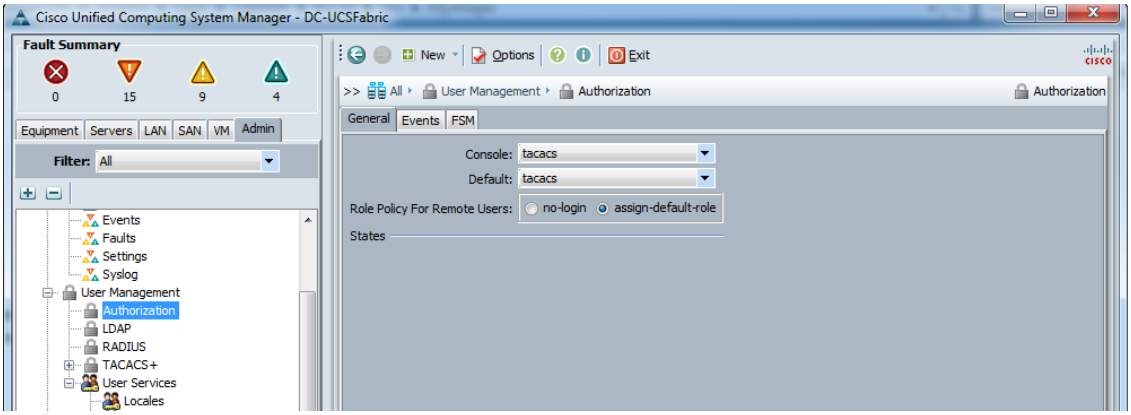
Add the Cisco Secure ACS server under the TACACS+ protocol option, as shown in Figure 5-41.

Figure 5-41 Adding the Cisco Secure ACS Server



Select **tacacs** from the Console and Default dropdown menus on the Authorization page, as shown in Figure 5-42.

Figure 5-42 Authorization—Selecting Console and Default Settings



On the TACACS+ server, create custom attributes defining the desired role for the user or group accessing the Cisco UCS Manager (see Figure 5-43):

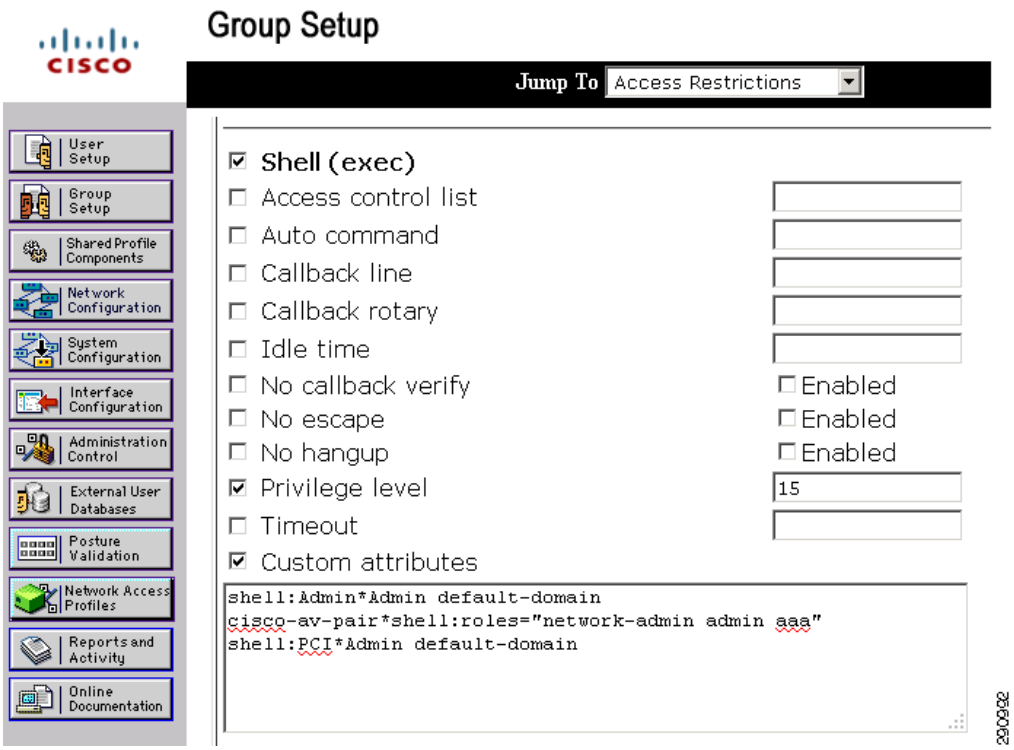
- TACACS+ custom attributes for UCS Manager:

```
cisco-av-pair*shell:roles="admin aaa"
```

- If combined with other systems roles, such as for the Nexus;

```
cisco-av-pair*shell:roles="network-admin admin aaa"
```

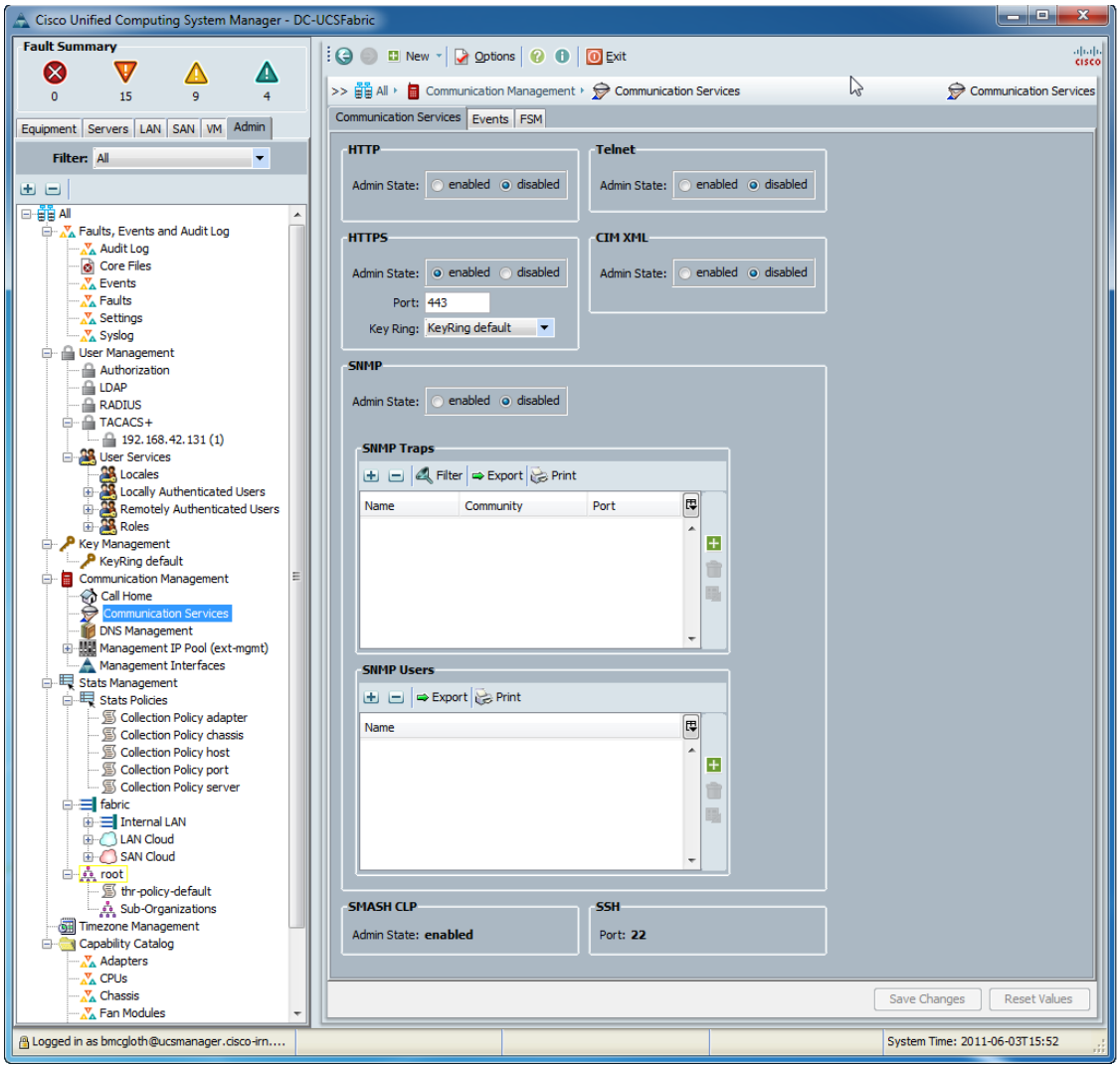
Figure 5-43 Group Configuration Page on TACACS+ Server



Local individual user accounts can be configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration as specified in established policies for passwords.

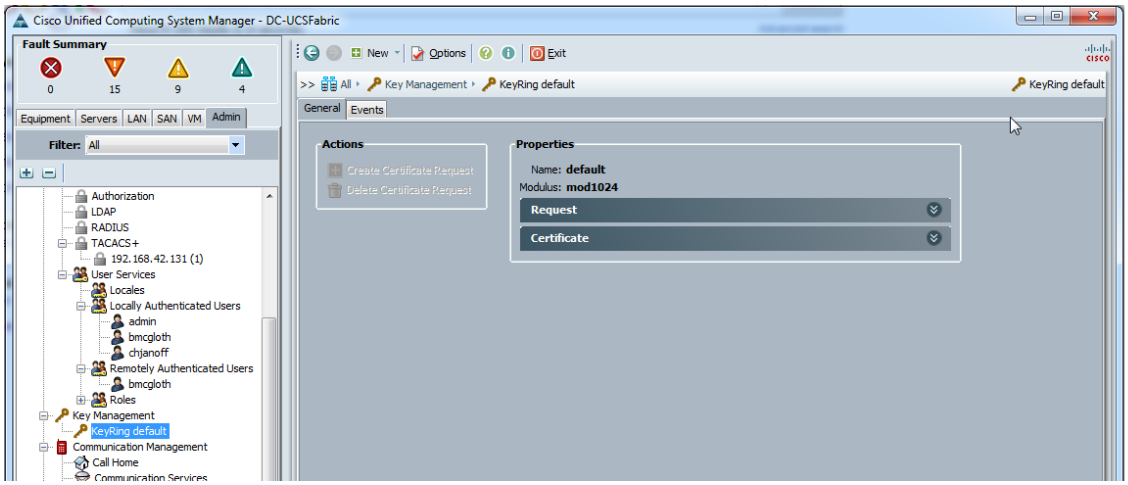
To secure authentication information and management of the UCS Manager, addressing Safeguard 164.308(a)(1)(i) Security Management, the Cisco UCS allows for the disabling of non-secure administrative interfaces. Figure 5-44 shows that the secure management protocols of SSH and HTTPS for administration. Telnet, HTTP, and other unused protocols are disabled.

Figure 5-44 Secure Management Protocols



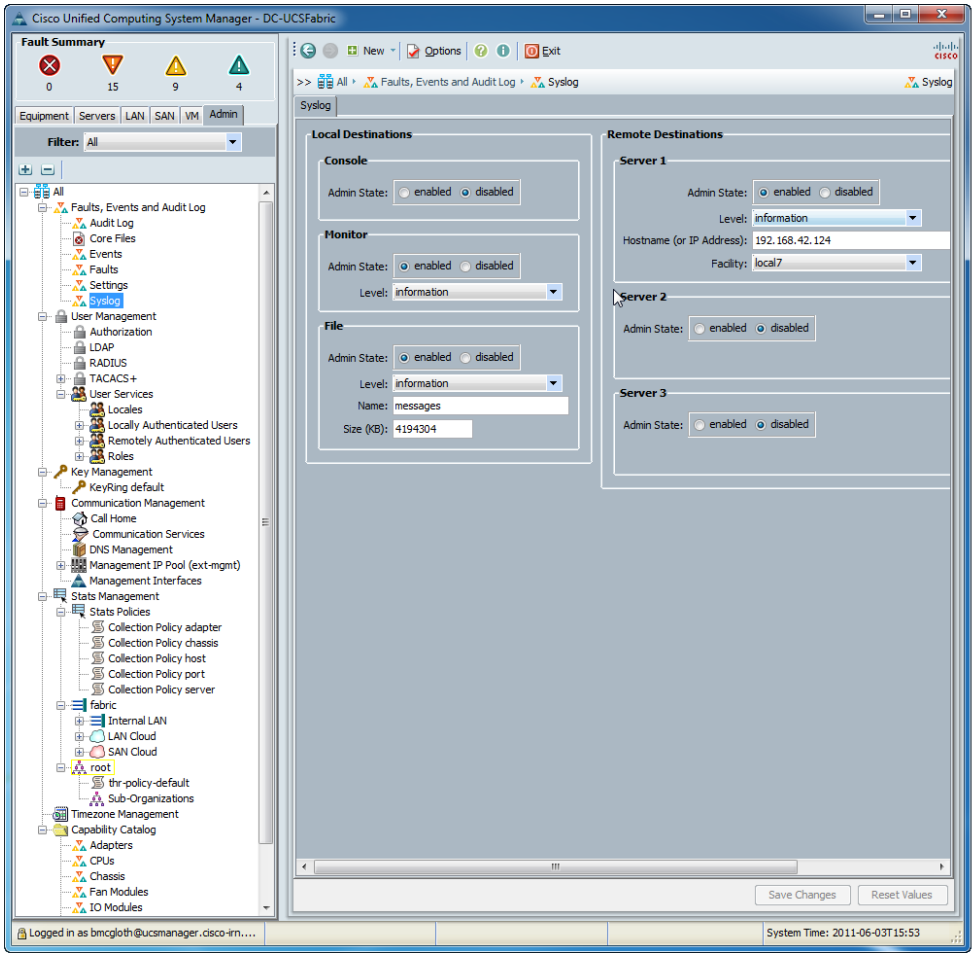
Cisco UCS uses strong encryption for SSH and HTTPS connections. Encryption keys are created and managed under the Key Management feature. (See Figure 5-45.)

Figure 5-45 1024-Bit Mod Key Default Keyring



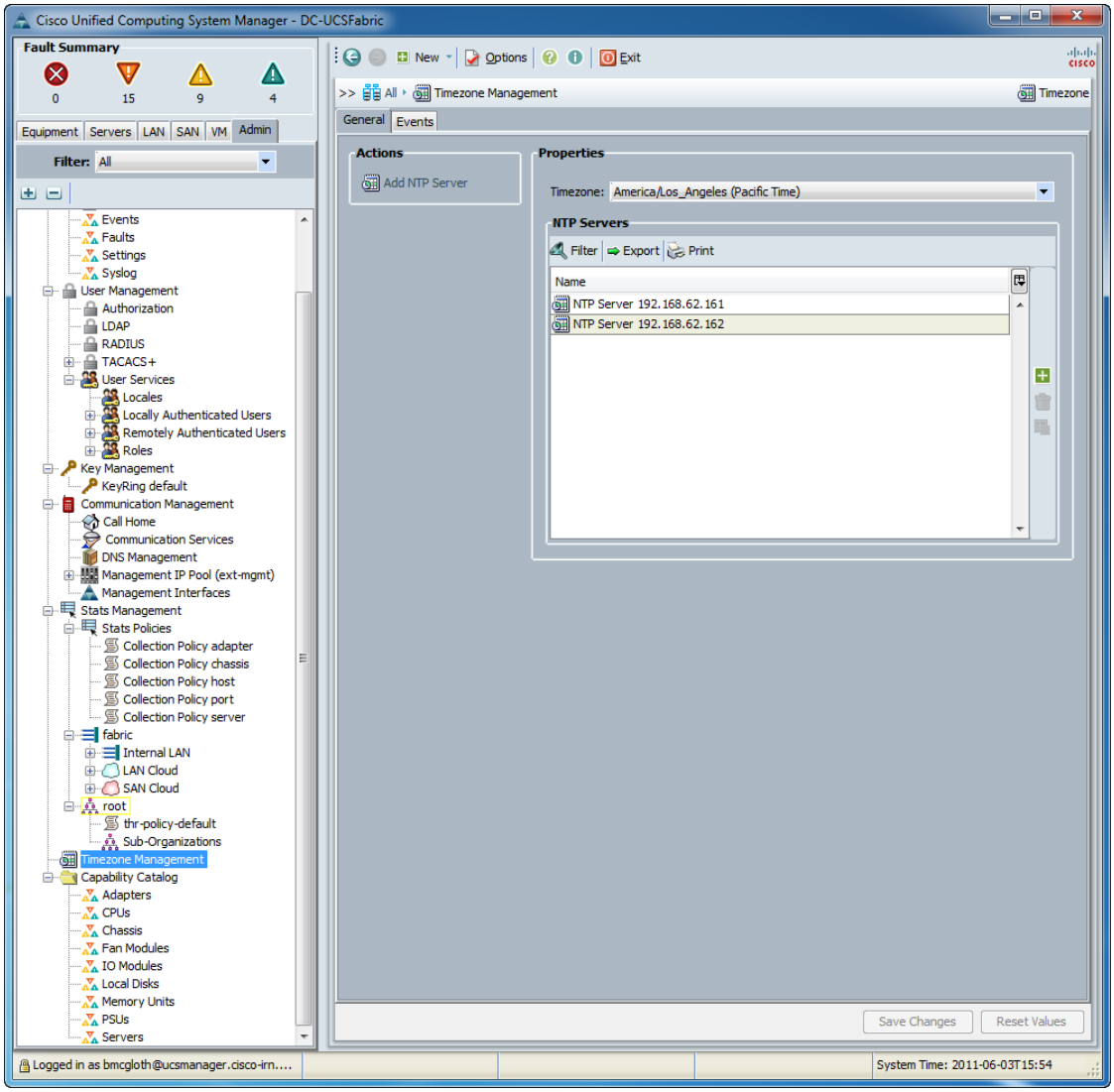
To address the Incident Response and Auditing HIPAA Safeguards identified above, Cisco UCS can be configured to send its data to the RSA enVision log management platform using the syslog function and/or SNMP traps. In the solution, only syslog was used. (SeeFigure 5-46).

Figure 5-46 Using Syslog



As a best practice, NTP is used to synchronize clocks among network devices (see Figure 5-47). This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

Figure 5-47 NTP Screen



Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Cisco UCS Express on Services Ready Engine

The Cisco Unified Computing System (UCS) Express and Services Ready Engine (SRE) is designed to allow organizations to securely deploy sensitive applications directly within the routing platform. By using the UCS E-series, organizations can remove legacy compute resources in the branch, saving space, energy, and operational costs.

Cisco UCS E-series is a converged networking, computing, and virtualization platform for hosting essential business applications in the clinic location. The SRE modules are router blades for the second generation of Cisco Integrated Services Routers (ISR G2) that provide the capability to host Cisco, third-party, and custom applications. A service-ready deployment model enables clinic applications to be provisioned remotely on the modules at any time. Cisco SRE modules have their own processors, storage, network interfaces, and memory, which operate independently of the host router resources and help ensure maximum concurrent routing and application performance.

Table 5-10 PHI HIPAA Assessment Summary—Cisco UCS Express

Models Assessed	
Cisco UCS Express version 1.1 on SRE900	
HIPAA Safeguards Addressed	
Administrative	**Standards/Implementation Specifications**
164.308	(a)(1)(i) Security Management Process
	(a)(3)(ii)(A) Authorization/Supervision
	(a)(4)(ii)(A) Isolating Clearing House Functions
	(a)(4)(i) Access Authorization
	(a)(5)(i) Log-in Monitoring
	(a)(6)(i) Security Incident Procedures
	(a)(6)(ii) Response and Reporting
Technical	**Standards/Implementation Specifications**
164.312	(a)(i) Access Control
	(b) Audit Controls
	(c)(1) Data Integrity
HIPAA Standards Failed	
No HIPAA standards were failed.	
HIPAA Implementation Specifications Failed	
No HIPAA implementation specifications were failed.	

Primary PHI Function

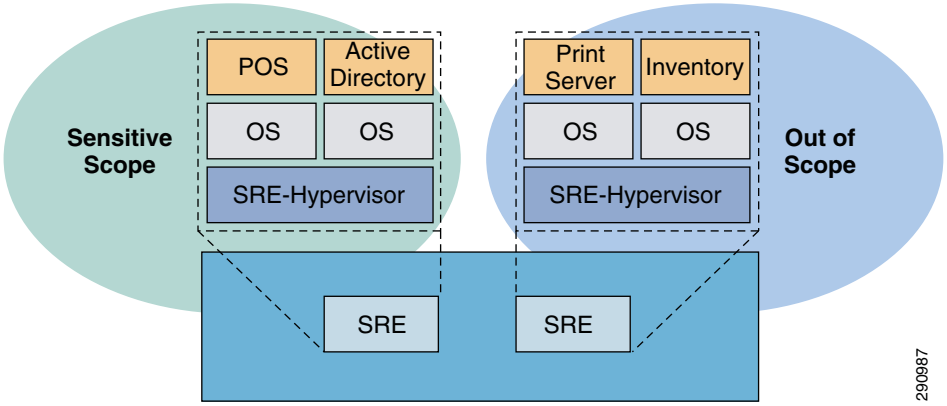
The primary function of the Cisco UCS Express is to securely host one primary compliance-related function per physical or virtual server.

It provides segmentation of sensitive applications from out-of-scope applications via physical and virtualization technology. UCS extends Layer 3 boundaries to virtual NIC and storage adapters within the chassis. Using VLANs and VSANs, Cisco UCS allows an organization to separate its sensitive ePHI (in-scope) from other non-sensitive data (out-of-scope).

Design Considerations

The major consideration when using Cisco UCS Express with sensitive applications is the security of the hypervisor. Verizon considers all hypervisors to be insecure because of vulnerabilities that may exist resulting in data leakage between VMs. Therefore, use separate Cisco UCS Express implementations when scoping. Although it is acceptable to mix non-sensitive applications onto a Cisco UCS Express deployment with sensitive applications, doing so brings those applications into scope and audit. (See Figure 5-48.)

Figure 5-48 Using UCS Express with Cisco SRE



Note Newer versions of UCS Express (version 1.5 +) enable central management of the VMware ESXi on Cisco UCS Express through vCenter (upgrade license required) as well as eliminate the Cisco console VM and local user management/VMware ESXi management restrictions. With the new release, Cisco UCS can manage users on VMware ESXi exactly as it would on a standalone VMware ESXi 4.1 server.

Note The Cisco UCS Express module comes installed with VMware ESXi. This is the primary function for the server module. Each module can host several independent operating systems as virtual servers. Each virtual server should have only one primary function.

- Cisco UCS Express requires the use of VLANs in the router. Depending on the deployment within the clinic, this may require the use of bridged virtual interfaces.
- Cisco UCS Express is based on VMware's ESXi and uses vSphere client for management.

HIPAA Assessment Detail—HIPAA Safeguards Addressed

All of the sample configurations of the UCS Express shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards

  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
  - §164.308(a)(4)(ii)(A) Isolating healthcare clearinghouse function. If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. Requirements addressed include: Access Control, Integrity, Incident Response and Auditing.
  - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
  - §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4). Requirements addressed include: Access Control and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical Safeguards.
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. Requirements addressed include: Auditing.
  - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
  - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
  - §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4). Requirements addressed include: Access Control and Auditing.
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.308(a)(6)(i) Response and Reporting. Implement policies and procedures to address security incidents. Requirements addressed include: Incident Response and Auditing.

  - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.

- Integrity—Protect electronic protected health information from improper alteration or destruction as required by HIPAA Technical safeguards.
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.312(c)(1) Data Integrity. Implement policies and procedures to protect health information from improper alteration or destruction.

Sample Configuration

Cisco UCS servers are able to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership. Cisco UCS Express includes extensive controls for defining user privileges and by default denies access to all individuals without a system user ID. On the UCS server configuration of the ESX hypervisor is part of the vSphere and vCenter infrastructure.

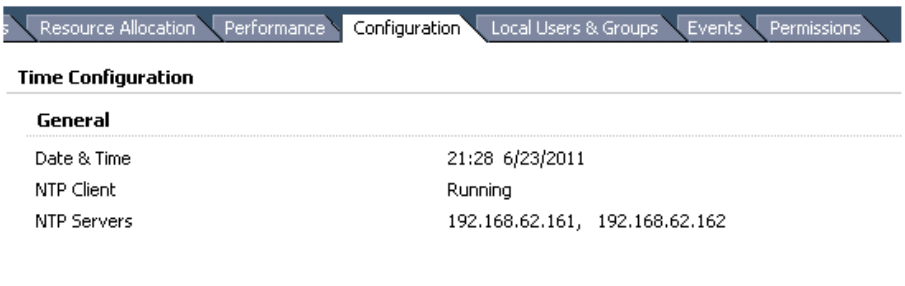
Local individual user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration as specified in established policies for passwords.

To secure authentication information and management of the UCS server, addressing Safeguard 164.308(a)(1)(i) Security Management, the UCS management console supports only HTTPS and SSH access.

Cisco UCS Express is designed to track and monitor all administrative user access, events such as profile creation, interface up/down, and device authentications. All of these events are sent to the vSphere and vCenter infrastructure.

NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers, as shown in Figure 5-49.

Figure 5-49 UCS E-Series NTP Servers



HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Administration

Authentication

Cisco Secure Access Control Server

Cisco Secure Access Control Server (ACS) was used as a central authentication system for the majority of products validated in this solution. It links user authentication to Windows Active Directory using group mapping that segments users based on their role and function.

Cisco Secure ACS is an access policy control platform that helps you comply with growing regulatory and corporate requirements. By using a single authentication method for all system devices, insight into who made changes is simplified for internal administration, assessors, and post-breach audits. It supports multiple scenarios simultaneously, including the following:

- Device administration—Authenticates administrators, authorizes commands, and provides an audit trail
- Remote access—Works with VPN and other remote network access devices to enforce access policies
- Wireless—Authenticates and authorizes wireless users and hosts and enforces wireless-specific policies
- Network admission control—Communicates with posture and audit servers to enforce admission control policies

Cisco Secure ACS lets you centrally manage access to network resources for a growing variety of access types, devices, and user groups. These key features address the current complexities of network access control:

- Support for a range of protocols including Extensible Authentication Protocol (EAP) and non-EAP protocols provides the flexibility to meet all your authentication requirements
- Integration with Cisco products for device administration access control allows for centralized control and auditing of administrative actions
- Support for external databases, posture brokers, and audit servers centralizes access policy control and lets you integrate identity and access control systems

Table 5-11 PHI HIPAA Assessment Summary—Cisco ACS

Models Assessed	
Cisco Secure Access Control Server	Release 4.2(1) Build 15 Patch 3
HIPAA Safeguards Addressed	

Table 5-11 PHI HIPAA Assessment Summary—Cisco ACS

Administrative	Standards/Implementation Specifications
164.308	(a)(1)(i) Security Management Process
	(a)(3)(ii)(A) Authorization/Supervision
	(a)(3)(ii)(C) Termination Procedures
	(a)(4)(ii)(B) Access Authorization
	(a)(4)(ii)(C) Access Establishment and Modification
	(a)(5)(ii)(C) Log-in Monitoring
	(a)(6)(ii) Response and Reporting
Technical	**Standards/Implementation Specifications**
164.312	(a)(2)(i) Unique User Identification
	(a)(2)(ii) Emergency Access Procedures
	(a)(2)(ii) Automatic Logoff
	(b) Audit Controls
	(d) Person or Entity Authentication
HIPAA Standards Failed	
No HIPAA standards were failed.	
HIPAA Implementation Specifications Failed	
No HIPAA implementation specifications were failed.	

Primary PHI Function

The primary function of Cisco Secure ACS is to securely authenticate users to the systems within the ePHI environment. The ACS allows for management of user access (authorization) to systems containing ePHI. Additionally, the ACS can prevent unauthorized devices from accessing systems containing ePHI and protect access from unauthorized locations. Users can be assigned to groups and, based on privilege levels, have access to only the information they require for their job function.

HIPAA Assessment Detail—HIPAA Safeguards Addressed

HIPAA safeguards are spread across multiple categories. ACS allows healthcare-covered entities and business associates to meet access control safeguards in the Administrative and Technical categories. The access control can be applied to both internal and external users that access ePHI data.

All of the sample configurations of the ACS shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations it might be accessed. Requirements addressed include: Access Control and Auditing.

  - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
  - §164.308(a)(4)(ii)(C) Access Establishment and Modification. Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. Requirements addressed include: Access Control, Incident Response, and Auditing.
  - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
  - §164.312(a)(2)(ii) Automatic logoff. Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. Requirements addressed include: Access Control.
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
  - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
  - §164.312(a)(2)(i) Unique User Identification. Assign a unique name and/or number for identifying and tracking user identity. Requirements addressed include: Access Control and Auditing.
  - §164.312(a)(2)(ii) Emergency Access Procedures. Establish (and implement as necessary) procedures for obtaining necessary ePHI during an emergency. Requirements addressed include: Access Control.
  - §164.312(d) Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. Requirements addressed include: Access Control and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical Safeguards.
  - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. Requirements addressed include: Auditing.

Design Considerations

- Cisco Secure ACS has been configured to authenticate individual users using Active Directory (AD). This is accomplished by creating user groups in AD and mapping them to role-based groups in Cisco Secure ACS. This provides the granularity of secure authentication needed to address the HIPAA specification.
- The solution used the windows versions of Cisco Secure ACS. The CSA client was installed to protect and alert on unauthorized access of the log and audit trail.
- Remove the default accounts for administration.
- Enable HTTPS and disable HTTP.

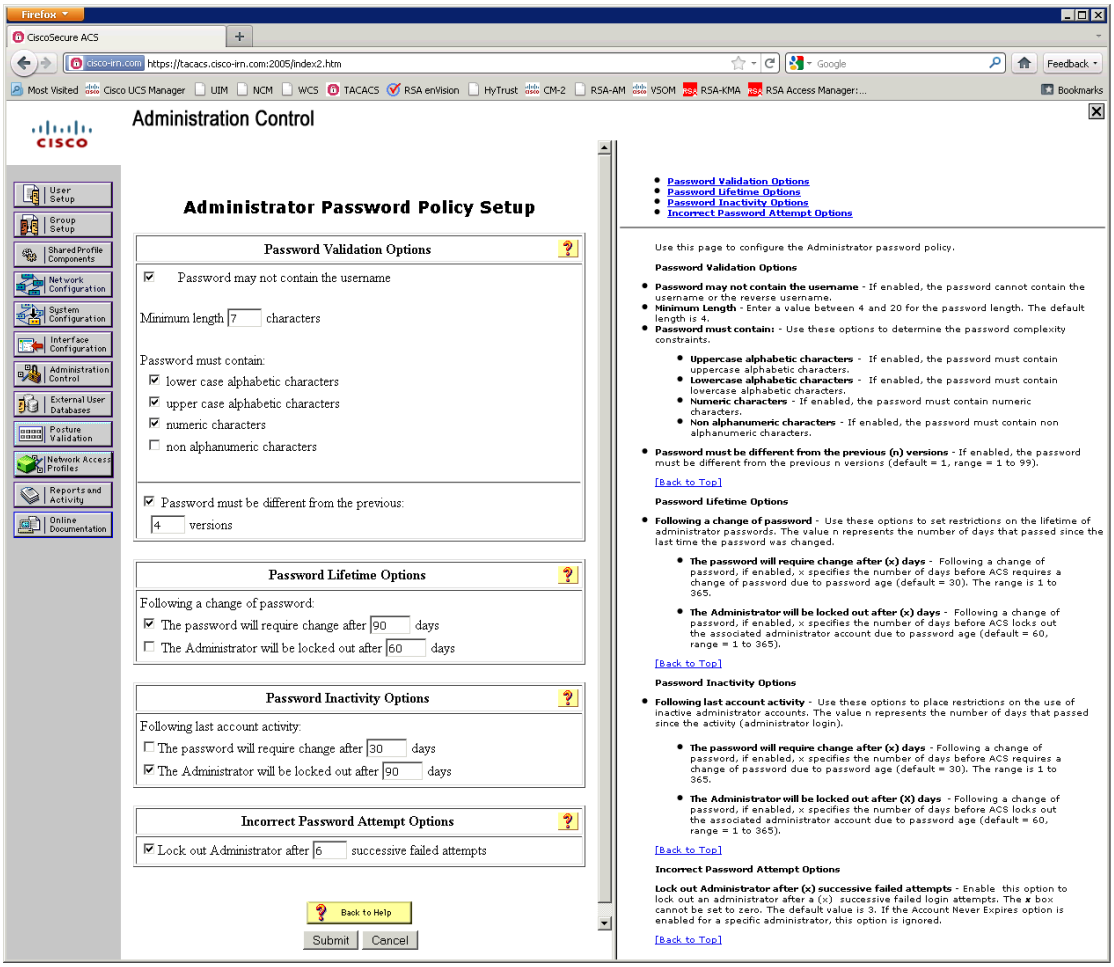
User authentication services for Cisco Secure ACS are linked to a centralized Active Directory user database. When personnel are added or removed from Active Directory, their access to infrastructure is similarly affected addressing Safeguard 164.308(a)(3)(ii)(C) Termination Procedures.

Sample Configuration

Cisco ACS is designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through Cisco ACS and ISE via LDAP, RADIUS, and TACACS+ services enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership.

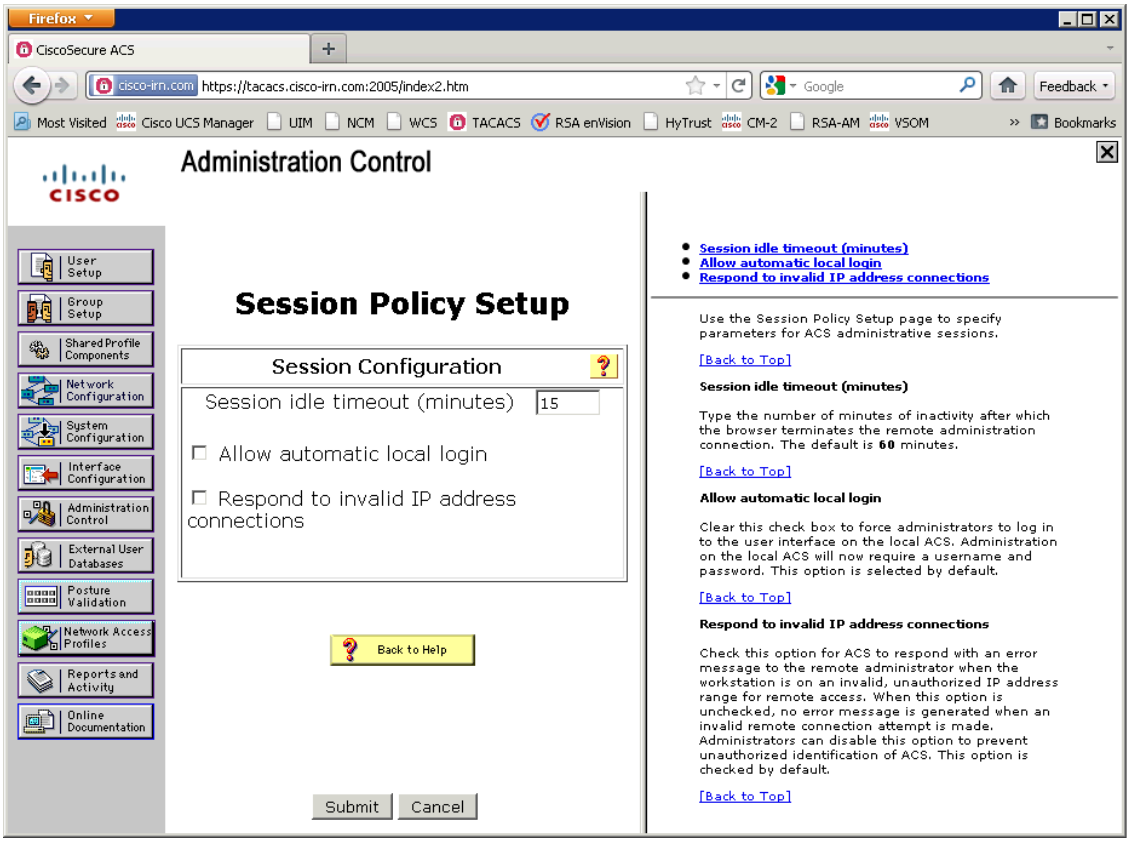
Cisco Secure ACS supports the creation of local administrative users. Each user must be assigned a unique ID. Cisco Secure ACS password policy enables setting of an inactivity option where an administrator is locked out after a specified period of inactivity determined by company policies. Local administrator user accounts in Cisco Secure ACS require the setting of a password according to the password requirements, as shown in Figure 5-50. By default, Cisco Secure ACS requires another administrator to re-enable locked out accounts.

Figure 5-50 Administrator Password Requirements



HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of automatic logoff options. Cisco Secure ACS supports session policies under the Administration Control/Session tab. The default session timeout is 60 minutes. It is a best practice to change the session timeout to 15 minutes, as shown in Figure 5-51.

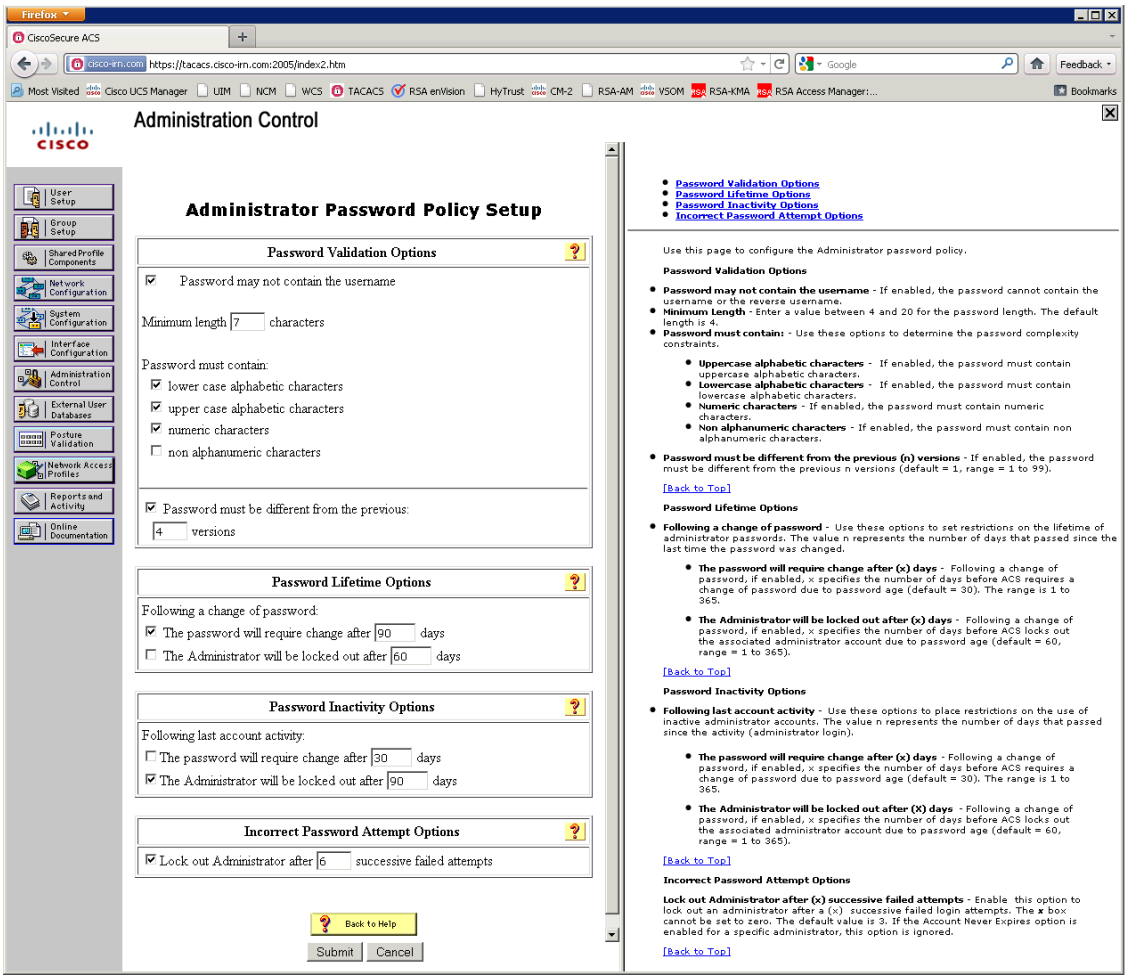
Figure 5-51 Session Timeout



To address the Incident Response and Auditing HIPAA Safeguards identified above, Cisco Secure ACS can be configured to send its log data to the RSA enVision log management platform. The configuration procedure is documented in the RSA enVision Event Source Configuration Guide for Cisco Secure ACS, which can be found at RSA Secure Care Online (https://knowledge.rsasecurity.com/).

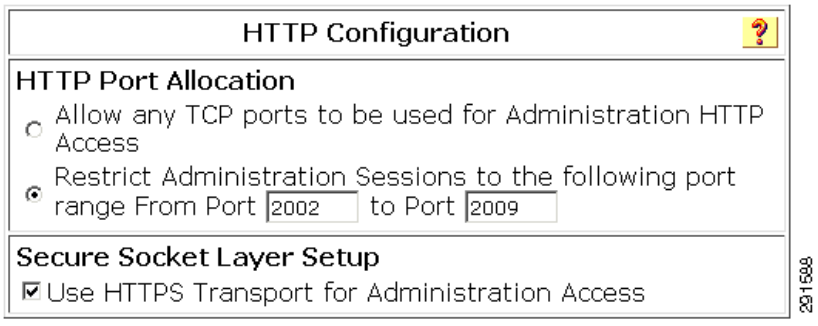
RSA enVision requires that specific attributes for each reporting function to be specified and configured in a particular order. Figure 5-52 shows the required items for generating Syslog Passed Authentications. Settings for other event types are available in the RSA enVision Event Source Configuration Guide for Cisco Secure ACS.

Figure 5-52 Syslog for Passed Authentications



To secure authentication information and management of the ACS server, addressing Safeguard 164.308(a)(1)(i) Security Management, the ACS management console was configured to support HTTPS access, with HTTP access disabled. Cisco Secure ACS is configured to use SSL as a highly secure management portal technology (see Figure 5-53). Cisco Secure ACS employs port hopping to a random high port for secured communication transport.

Figure 5-53 HTTP Configuration



As a best practice, NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. Time synchronization for Windows servers is specified through the domain policy. Servers synchronize their clocks with the domain controller, which in turn is synchronized using NTP. This implementation of Cisco ACS was Windows-based.

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

RSA Authentication Manager

RSA Authentication Manager is the management component of the RSA SecurID®, a two-factor authentication solution, which provides a much more reliable level of user authentication than reusable passwords. SecurID authentication is based on something you know (a password or PIN) and something you have (an authenticator). As the management component, RSA Authentication Manager is used to verify authentication requests and centrally administer authentication policies for enterprise networks.

Table 5-12 PHI HIPAA Assessment Summary—Cisco RSA Authentication Manager

Models Assessed	
RSA Authentication Manager 7.1 Service Pack 2	
HIPAA Safeguards Addressed	
Administrative	**Standards/Implementation Specifications**
164.308	(a)(1)(i) Security Management Process
	(a)(3)(i) Authorization/Supervision
	(a)(4)(i) Access Authorization
	(a)(5)(i) Log-in Monitoring
	(a)(6)(i) Security Incident Procedures
	(a)(6)(ii) Response and Reporting
Technical	**Standards/Implementation Specifications**
164.312	(a)(i) Access Control
	(b) Audit Controls
	(c)(1) Data Integrity
HIPAA Standards Failed	
No HIPAA standards were failed.	
HIPAA Implementation Specifications Failed	
No HIPAA implementation specifications were failed.	

Primary PHI Function

The primary function of RSA Authentication Manager is to securely authenticate remote users using two-factor authentication.

Design Considerations

RSA Authentication Manager stores and processes highly sensitive authentication information and should be deployed and operated in a secure manner. Detailed recommendations are found in the RSA Authentication Manager Security Best Practices Guide, which can be downloaded from RSA Secure Care Online (https://knowledge.rsasecurity.com/).

HIPAA Assessment Detail—HIPAA Safeguards Addressed

All of the sample configurations of the RSA Authentication Manager shown below were used to meet the following list of satisfied controls:

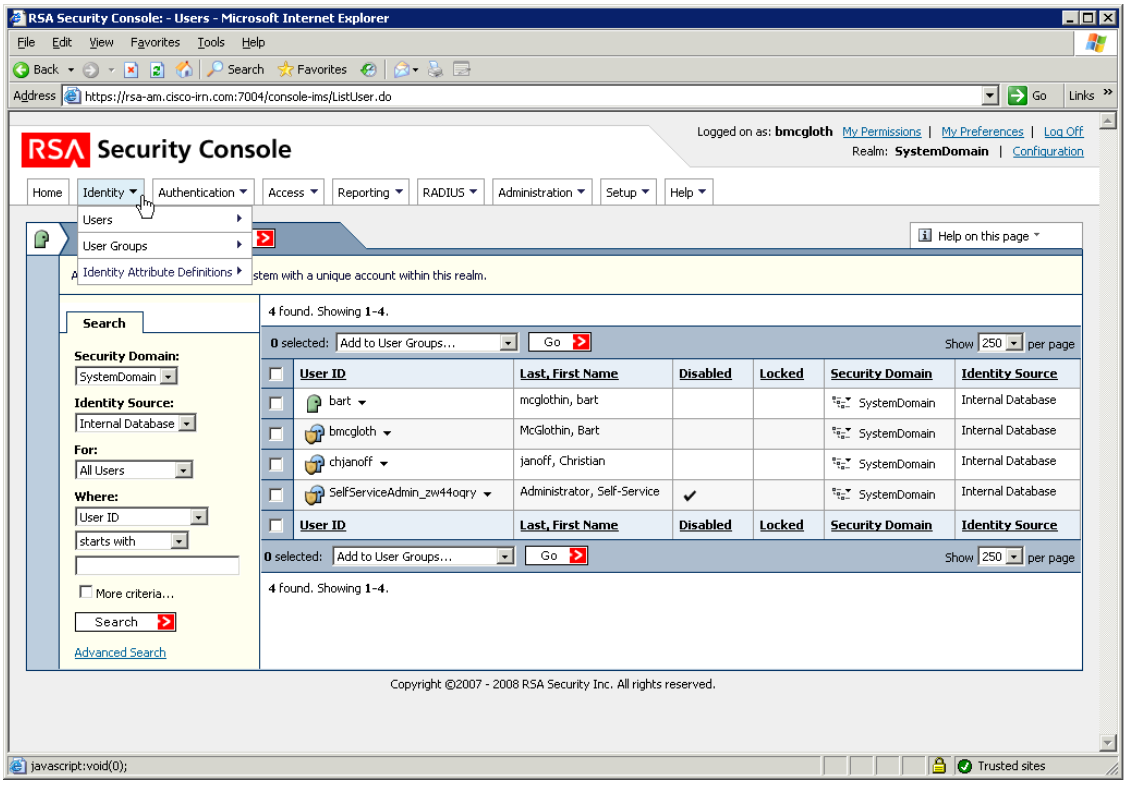
- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
  - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
  - §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
  - §164.308(a)(6)(i) Security Incident Procedures. Implement policies and procedures to address security incidents.
  - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
  - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. Requirements addressed include: Auditing.
  - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
- Integrity—Protect electronic protected health information from improper alteration or destruction as required by HIPAA Technical safeguards.

– §164.312(c)(1) Data Integrity. Implement policies and procedures to protect health information from improper alteration or destruction.

Sample Configuration

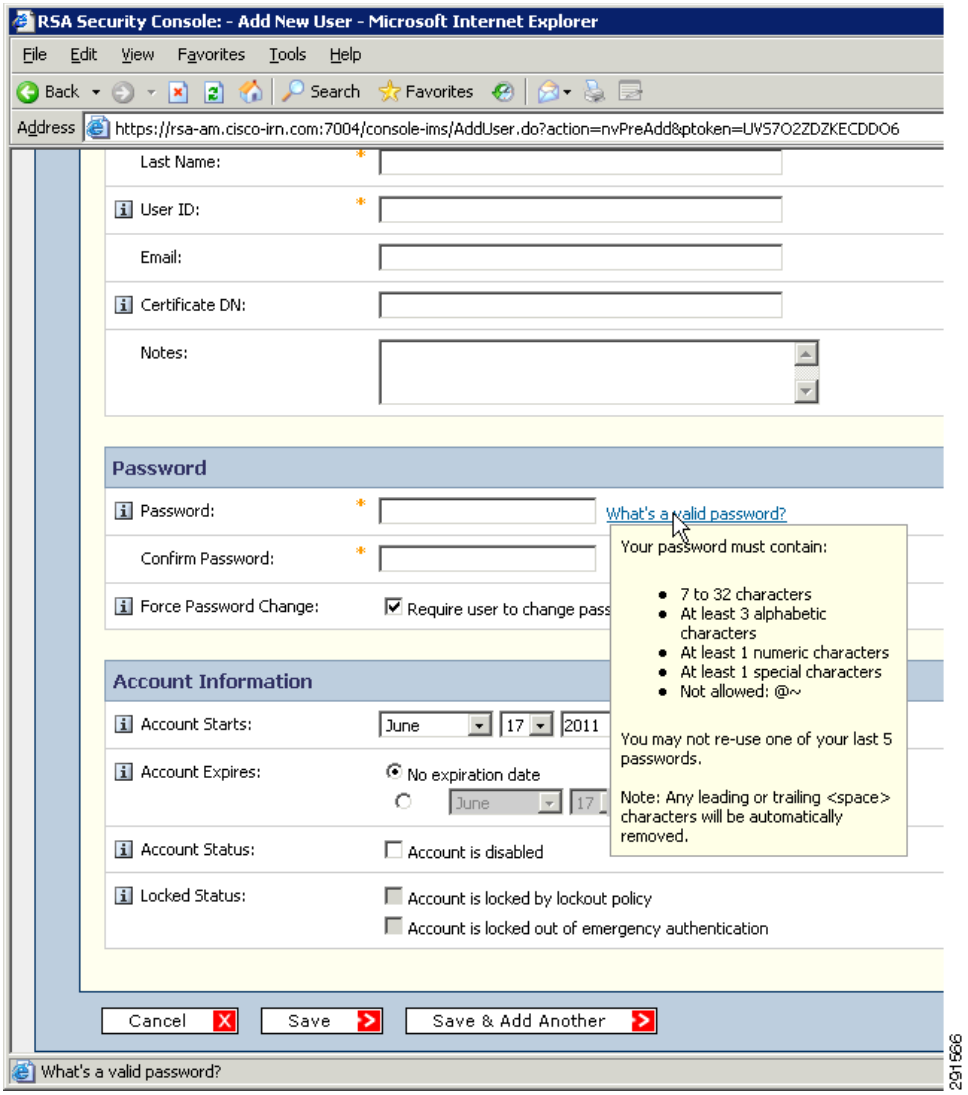
RSA Authentication Manager has powerful access control capabilities to limit, track, and monitor all user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. RSA Authentication Manager protects epHI data based on user role or group membership. Users and groups are created under the Identity tab of the Security console, as shown in Figure 5-54.

Figure 5-54 Users and Groups



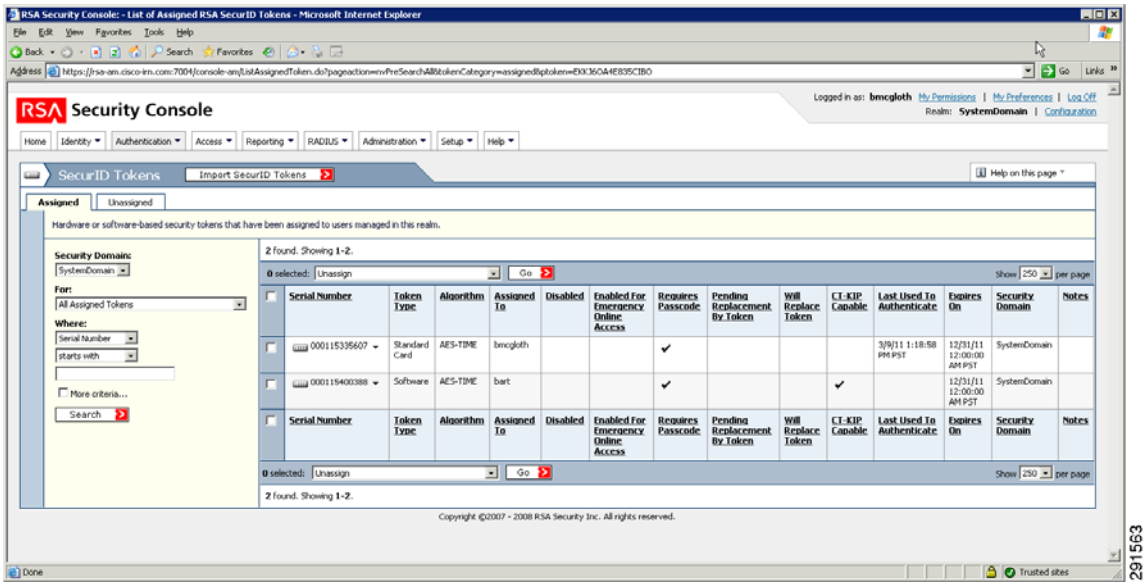
Local individual user accounts are configured in the event that the centralized authentication server cannot be reached, and support advanced policies regarding password rotation and expiration as can be configured as necessary. Local user accounts in RSA Authentication Manager require setting of a password according to the assigned password policy as shown in Figure 5-55.

Figure 5-55 User Password Requirements Based on Policy



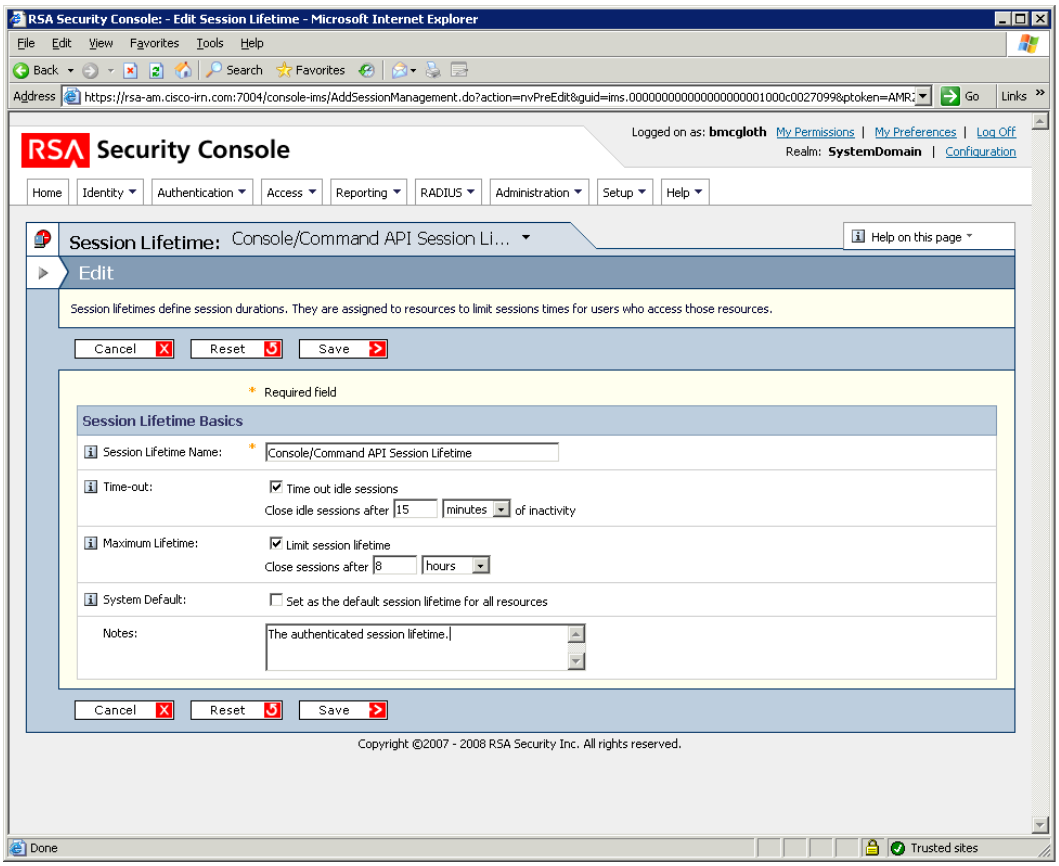
Additional authentication tokens can also be assigned to each user, as shown in Figure 5-56.

Figure 5-56 Assigned Tokens



HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of automatic logoff options. RSA Authentication Manager supports session policies under the Access tab. Change the Session Time-out for the Console/Command API to 15 minutes from the default, as shown in Figure 5-57.

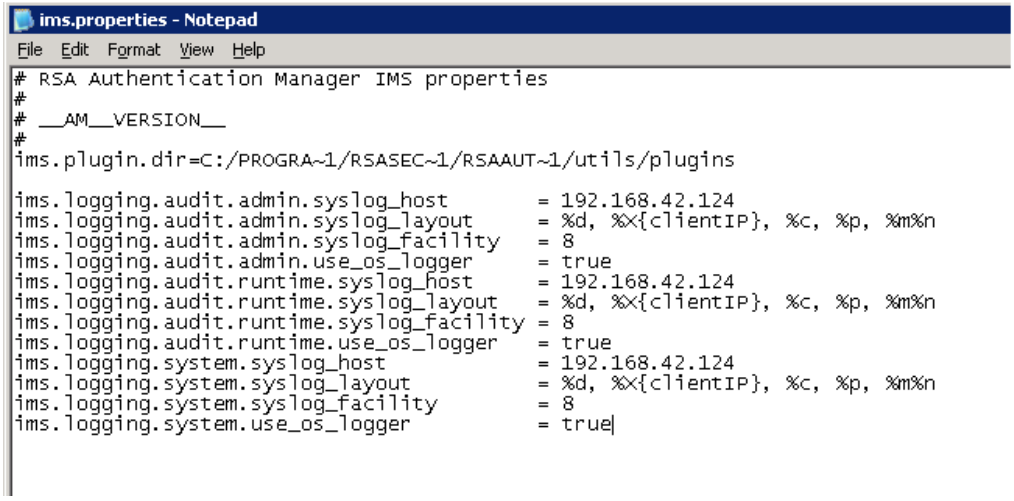
Figure 5-57 Session Lifetime for Console



To secure authentication information and management of the server, addressing Safeguard 164.308(a)(1)(i) Security Management, the management console supports only HTTPS access by default.

To address the Incident Response and Auditing HIPAA Safeguards identified above, RSA Authentication Manager can be configured to send its log data to the RSA enVision log management. The configuration procedure is documented in the enVision Event Source Configuration Guide for RSA Authentication Manager, which can be found at RSA Secure Care Online (https://knowledge.rsasecurity.com/). One step is editing the IMS.Properties file, as shown in Figure 5-58.

Figure 5-58 IMS Properties File



As a best practice, NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. Time synchronization for Windows servers is specified through the domain policy. Servers synchronize their clocks with the domain controller, which in turn is synchronized using NTP. This implementation was Windows-based.

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Cisco Identity Services Engine

The Cisco Identity Services Engine (ISE) allows for management of user access (authorization) to systems containing PHI. Additionally, the Access Control Server is designed to prevent unauthorized devices from accessing systems containing PHI and protect access from unauthorized locations. ISE is a security component that provides visibility and control into who and what is connected to the network. Cisco ISE allows organizations to embrace the rapidly changing business environment of mobility,

virtualization, and collaboration while enforcing compliance, maintaining data integrity and confidentiality, and establishing a consistent global access policy. Cisco ISE allows businesses to gain complete control over the access points into their networks. This includes all wired, wireless, and VPN network entry points.

Cisco ISE allow you to see what devices and users are on your network, and that those devices and users comply with your security policies via the following components:

- Cisco Identity Services Engine—A next-generation policy manager that delivers authentication, authorization, and accounting (AAA); posture; profiling; and guest management services on a single platform. The Cisco ISE automatically discovers and classifies endpoints, provides the right level of access based on identity, and provides the ability to enforce endpoint compliance by checking a device's posture. The Cisco ISE also provides advanced authorization and enforcement capabilities, including Security Group Access (SGA) through the use of security group tags (SGTs) and security group access control lists (ACLs). Administrators can centrally create and manage access control policies for users and endpoints in a consistent fashion, and gain end-to-end visibility into everything that is connected to the network.
- Cisco ISE Identity on Cisco Networking Infrastructure—Identity-based networking services on the Cisco routing, switching, and wireless infrastructure provides the ability to authenticate users and devices via features such as 802.1x, MAC authentication bypass, and web authentication. In addition, this same infrastructure is what enforces the appropriate access into parts of the network via VLANs, downloadable or named ACLs and security group ACLs.
- Client—Cisco AnyConnect is a software client that enables you to deploy a single 802.1x authentication framework to access wired and wireless networks while the Cisco NAC agent delivers endpoint posture information. The Cisco ISE architecture also supports native O/S supplicants.

The Cisco Identity Services Engine solution offers the following benefits:

- Allows enterprises to authenticate and authorize users and endpoints via wired, wireless, and VPN with consistent policy throughout the enterprise
- Prevents unauthorized network access to protect corporate assets
- Provides complete guest lifecycle management by empowering sponsors to on-board guests, thus reducing IT workload
- Discovers, classifies, and controls endpoints connecting to the network to enable the appropriate services per endpoint type
- Enforces security policies by blocking, isolating, and repairing noncompliant machines in a quarantine area without needing administrator attention
- Offers a built-in monitoring, reporting, and troubleshooting console to assist helpdesk operators and administrators streamline operations.

Figure 5-59 shows an example of a Cisco ISE-based LAN deployment.

Figure 5-59 Cisco ISE-Based LAN Deployment

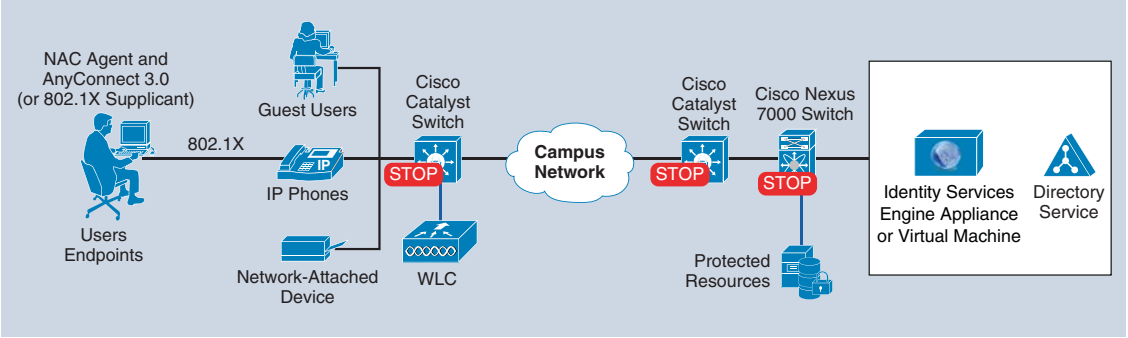


Table 5-13 PHI HIPAA Assessment Summary—Cisco ISE

Models Assessed	
Cisco Identity Service Engine version 1.0.3.377	
HIPAA Safeguards Addressed	
Administrative	**Standards/Implementation Specifications**
164.308	(a)(1)(i) Security Management Process
	(a)(3)(ii)(A) Authorization/Supervision
	(a)(4)(ii)(A) Isolating Clearing House Functions
	(a)(4)(ii)(B) Access Authorization
	(a)(4)(ii)(C) Access Est./Modification
	(a)(5)(ii)(C) Log-in Monitoring
	(a)(5)(ii)(D) Password Management
	(a)(6)(i) Security Incident Procedures
	(a)(6)(ii) Response and Reporting
Technical	**Standards/Implementation Specifications**
164.312	(a)(i) Access Control
	(b) Audit Controls
	(a)(2)(ii) Emergency Access Procedures
	(a)(d) Personal Entity Authentication
HIPAA Standards Failed	
No HIPAA standards were failed.	
HIPAA Implementation Specifications Failed	
No HIPAA implementation specifications were failed.	

Primary PHI Function

Cisco ISE identity features are designed to detect and prevent rogue wireless devices from connecting to in-scope PHI networks; in addition, Cisco ISE locks down publicly accessible network ports to only authorized devices and users.

The Identity Services Engine allows for management of user access (authorization) to systems containing PHI. Additionally, the Access Control Server can prevent unauthorized devices from accessing systems containing PHI and protect access from unauthorized locations.

Identity Services Engine logs can be used to identify unauthorized attempts to connect to systems containing PHI to help meet the supervision requirements.

Design Considerations

For the purposes of this guide, Cisco ISE is configured to authenticate individual users and ISE Admin users using Active Directory (AD). Cisco ISE is also used to profile and assess the posture of individual wired and wireless devices to ensure that they comply with the HIPAA standard. Cisco ISE relies on TrustSec wired and wireless identity features such as 802.1x, MAB, and web portal authentication on Cisco infrastructure to collect user identity information. It relies on the Cisco ISE NAC agent and the Cisco ISE profiler engine to collect posture and profiling information from devices.

Note the following ISE configuration best practices for HIPAA compliance:

- The solution tested used the virtual machine appliance version of Cisco ISE running on an ESX platform.
- The default accounts for administration are removed.
- ISE only supports HTTPS and SSH access
- Cisco ISE communicates with the Cisco switches and wireless controllers using RADIUS.
- Cisco ISE can use dynamic VLAN and port or VLAN access control rules to provide HIPAA segmentation of a network. For example, members of the HIPAA active directory group are automatically moved to the HIPAA VLAN when they connect to the network. Cisco ISE can then apply strong access lists to this VLAN or directly to the user switch port to accomplish segmentation.
- Access control rule sets must adhere to a “least amount of access necessary” policy. Rules must be defined by specific source/destination addressing and TCP/UDP ports required for the PHI data environment.
- Configure appropriate banner messages on login, incoming, and exec modes of the router. The login banner warning should not reveal the identity of the company that owns or manages the router. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- The Cisco ISE system is configured to be compliance with all of the access controls, logging controls, and other general system controls required by HIPAA.

HIPAA Assessment Detail—HIPAA Safeguards Passed

All of the sample configurations of the Cisco ISE shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.

  - §164.308(a)(4)(ii)(A) Isolating healthcare clearinghouse function. If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
  - §164.308(a)(4)(ii)(C) Access Establishment and Modification. Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. Requirements addressed include: Access Control, Incident Response, and Auditing.
  - §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).
  - §164.312(d) Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. Requirements addressed include: Access Control and Auditing.
  - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
  - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
  - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
  - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. Requirements addressed include: Auditing.
  - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
  - §164.312(d) Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. Requirements addressed include: Access Control and Auditing.

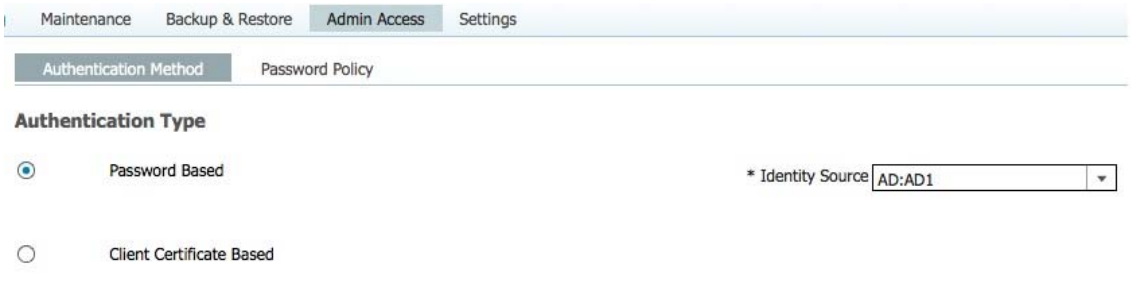
Sample Configuration

Cisco ISE is designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via

LDAP and RADIUS services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership.

Figure 5-60 shows admin authentication configured to use Active Directory.

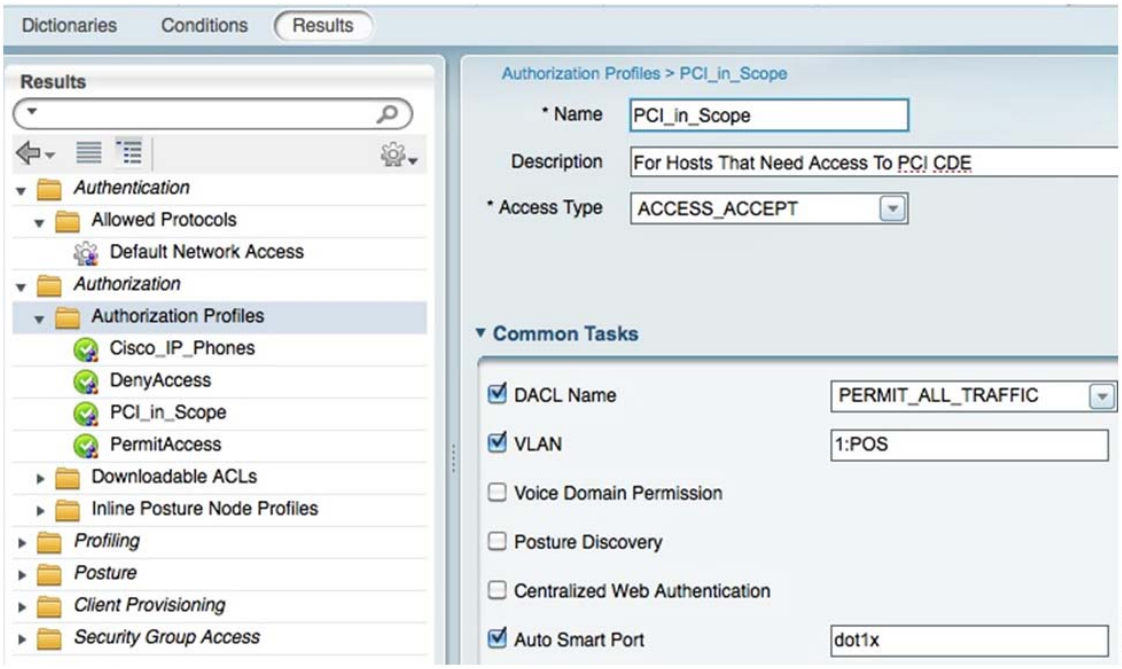
Figure 5-60 Admin Access Using Active Directory for Authentication



Cisco ISE cntrols access so that only privileged users can access the ePHI environment. This is done using the authentication credentials supplied by the wired and wireless infrastructure, along with the AD attributes of a user connecting to the network. Based on a Cisco ISE authorization profile match, that user is put onto the proper VLAN and given a group-specific port access control list to control where they can go on the network. Additionally, a Cisco SmartPort macro can be run on the switchport for proper configuration.

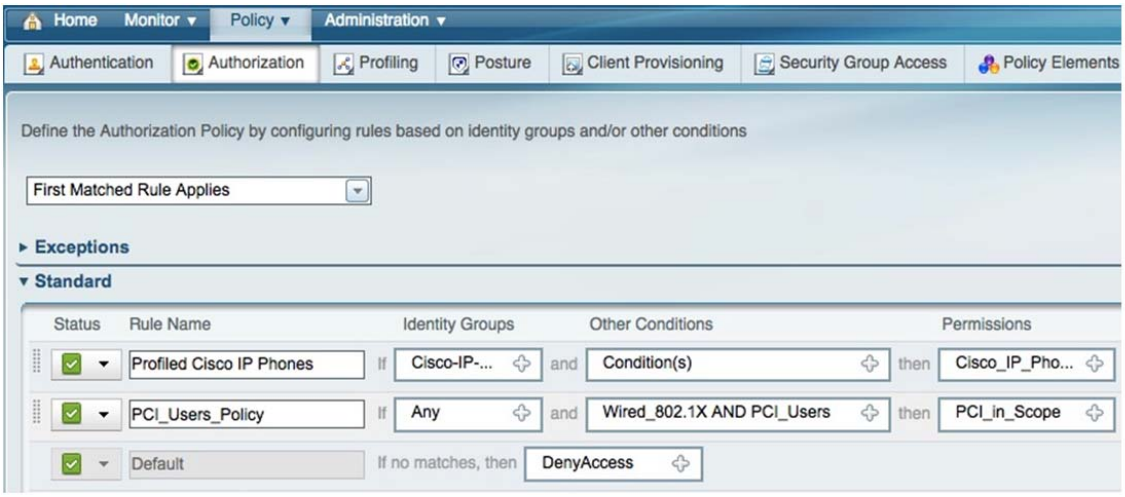
Figure 5-61 shows the Authorization Profiles screen.

Figure 5-61 Authorization Profiles



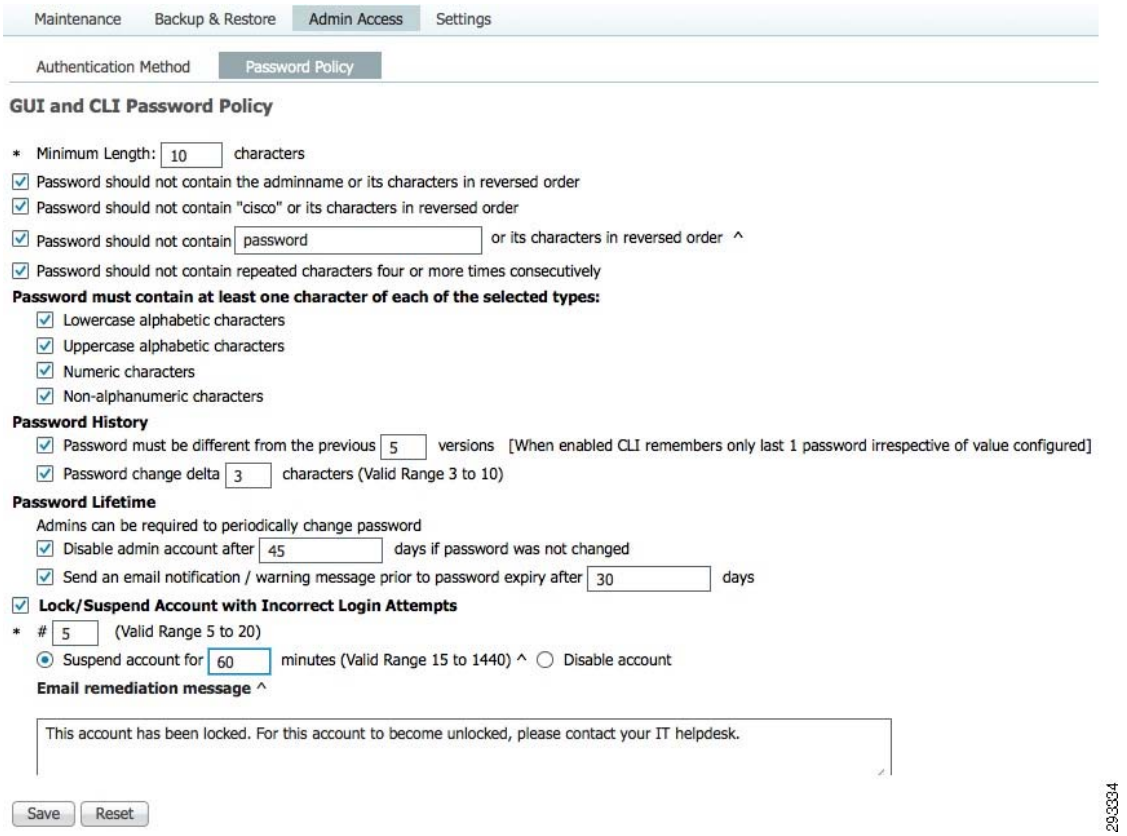
If Cisco ISE does not explicitly match an authorization policy as shown in Figure 5-62, network access is denied.

Figure 5-62 Authorization Policy



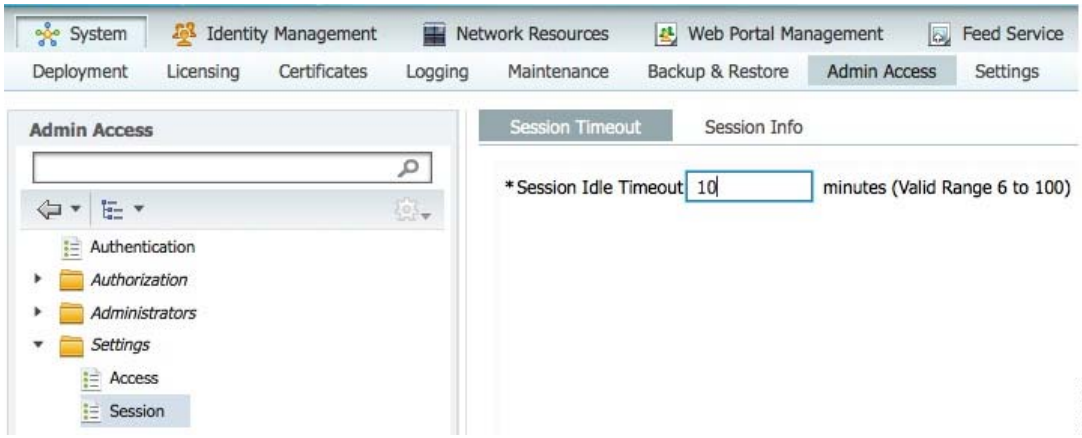
Local individual user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration as specified in established policies for passwords. The passwords used for these accounts can be tailored by editing of the Password Policy to match corporate requirements as shown in Figure 5-63.

Figure 5-63 ISE Admin Password Policy Settings



HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of automatic logoff options. Cisco ISE supports session idle timeout under the Administration Access/Session tab. It is a best practice to change the session timeout to 15 minutes, as shown in Figure 5-64, which will re-authenticate both admin users and RADIUS users.

Figure 5-64 Admin Access



To secure authentication information and management of the ISE server, addressing Safeguard 164.308(a)(1)(i) Security Management, the ISE management console supports only HTTPS access.

Additionally, Cisco ISE NAC capabilities can be configured on the clinic and hospital switches to automate the verification of approved devices being attached to the network. In addition to configuring the ISE authentication services in the data center, adding the following configurations to all switch and switch interface ports where ISE network access control is required. In most cases, every access switch port in your network should be protected using ISE. However, as a minimum, any switch port that could potentially let a host find its way to the ePHI security domain should be protected by Cisco ISE.

Pre-requirements for ISE NAC (domain name, name server, time settings, crypto keys):

```
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
Crypto key generate rsa 1024
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162
clock timezone PST -8
clock summer-time PDT recurring
!
! ----Configurations to add for NAC ----
!
aaa new-model
!
!
aaa authentication dot1x default group radius local
aaa authorization network default group radius
aaa authorization auth-proxy default group radius
aaa accounting dot1x default start-stop group radius
!
aaa server radius dynamic-author
client 192.168.42.111
server-key 7 <removed>
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server dead-criteria time 5 tries 3
```

```
radius-server host 192.168.42.111 auth-port 1812 acct-port 1813 key 7 <removed>
radius-server vsa send accounting
radius-server vsa send authentication
!
authentication mac-move permit
!
!
ip device tracking
ip admission name ise proxy http inactivity-time 60
!
cts sxp enable
cts sxp default source-ip 10.10.111.13 {use Switch Management IP}
!
dot1x system-auth-control
!
fallback profile ise
ip access-group ACL-DEFAULT in
ip admission ise
!
! ----Auto Smart Ports Macro method for port configurations-------
!
macro name dot1x
switchport access vlan 11
switchport mode access
switchport voice vlan 13
ip arp inspection limit rate 1000
ip access-group ACL-DEFAULT in
authentication event fail action next-method
authentication host-mode multi-auth
authentication open
authentication order dot1x mab webauth
authentication priority dot1x mab
authentication port-control auto
authentication timer reauthenticate server
authentication timer inactivity server
authentication violation restrict
authentication fallback ise
mab
snmp trap mac-notification change added
dot1x pae authenticator
dot1x timeout tx-period 5
```

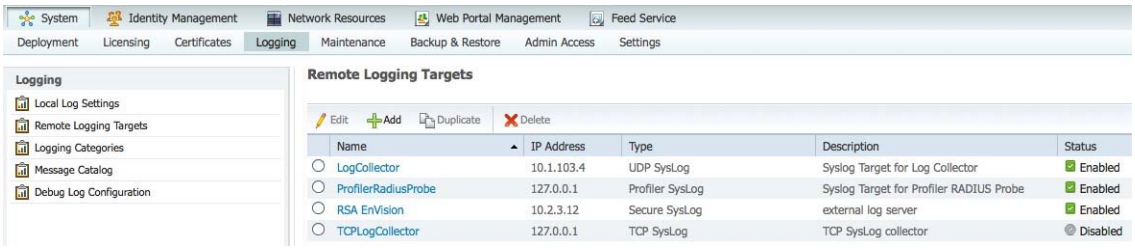
Methods that may be used in the process include, but are not limited to, wireless network scans, physical site inspections, Network Access Control (NAC), or wireless IDS/IPS.

Cisco ISE Identity features were enabled on the wired infrastructure to authenticate users and devices. The Cisco ISE Policy Manager was configured to not allow an unauthorized device to connect to the wired network. Cisco ISE was configured to alert and mitigate this threat.

Cisco ISE was configured to profile all devices connected to the network. Any devices detected were allowed only if they were in the approved list. All wired ports were set up to authenticate and posture-assess users and devices connecting to the network switches. The device posture assessment included checks for the setup of peer-to-peer wireless network and the setup of a wireless card as an access point on the device. If either of these were true, the device would be denied network access.

To address the Incident Response and Auditing HIPAA Safeguards identified above, Cisco ISE can be configured to send its log data to the RSA enVision log management platform. Figure 5-65 shows the configuration of logging servers.

Figure 5-65 Remote Logging Targets



As a best practice, NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. Cisco ISE uses NTP to meet these requirements by implementing the following configuration statement:

```
ntp server 192.168.62.161 192.168.62.162
```

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Management

Cisco Prime LAN Management Solution (LMS)

Cisco Prime LAN Management Solution (LMS), a part of Cisco Prime Infrastructure, delivers powerful network lifecycle management by simplifying the configuration, compliance, monitoring, troubleshooting, and administration of Cisco networks. Cisco Prime LMS offers end-to-end management for Cisco's latest business-critical technologies and services such as Medianet, Cisco ISE, and Cisco EnergyWise while complying with corporate and regulatory requirements.

Table 5-14 PHI HIPAA Assessment Summary—Cisco LMS

Models Assessed	
Cisco Prime Management Solution	
HIPAA Safeguards Addressed	
Administrative	**Standards/Implementation Specifications**
164.308	(a)(1)(i) Security Management Process
	(a)(3)(i) Authorization/Supervision
	(a)(4)(i) Access Authorization
	(a)(5)(i) Log-in Monitoring
	(a)(6)(i) Response and Reporting
Technical	**Standards/Implementation Specifications**
164.312	(a)(i) Access Control
	(b) Audit Controls
HIPAA Standards Failed	
No HIPAA standards were failed.	
HIPAA Implementation Specifications Failed	
No HIPAA implementation specifications were failed.	

Primary PHI Function

LMS simplifies compliance by ensuring that all of the devices across the network adhere to the security policy of the company. In addition, it will verify that device configurations; match templates, are synchronized, and includes a customized compliance dashboard to simplify the ongoing management for administrators.

Design Considerations

- Provide sufficient licenses to cover all devices in your network.
- Provide proper host system sizing including CPUs, memory, and storage for the selected operating system.
- Restrict access behind a firewall or access list to only those administrative clients that need access.
- Activate the NMC capability license for compliance audits.

Licensed/Unlicensed Compliance and Audit Reports

The following compliance and audit reports require a regulatory compliance management license:

- HIPAA Compliance Reports
- SOX (COBIT) Compliance Reports
- ISO/IEC 27002 Compliance Reports
- NSA Compliance Reports
- PCI DSS Compliance Reports
- DHS Checklist Reports
- DISA Checklists Report
- CIS Benchmarks

The following compliance and audit reports are supported by the LMS license alone and do not require a regulatory compliance management license:

- Service Reports
- Lifecycle Management Reports
- Vendor Advisory Reports
- Change Audit Reports

For compliance and audit license information, see the topic "Regulatory Compliance Management License in Administration with Cisco Prime LAN Management Solution 4.2.2".

The Compliance and Audit Report module uses the stored configurations within the LMS database and evaluates them against specifically defined criteria of the selected devices.

HIPAA Assessment Detail—HIPAA Safeguards Passed

All of the sample configurations of the LMS shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
  - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
  - §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).
  - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.

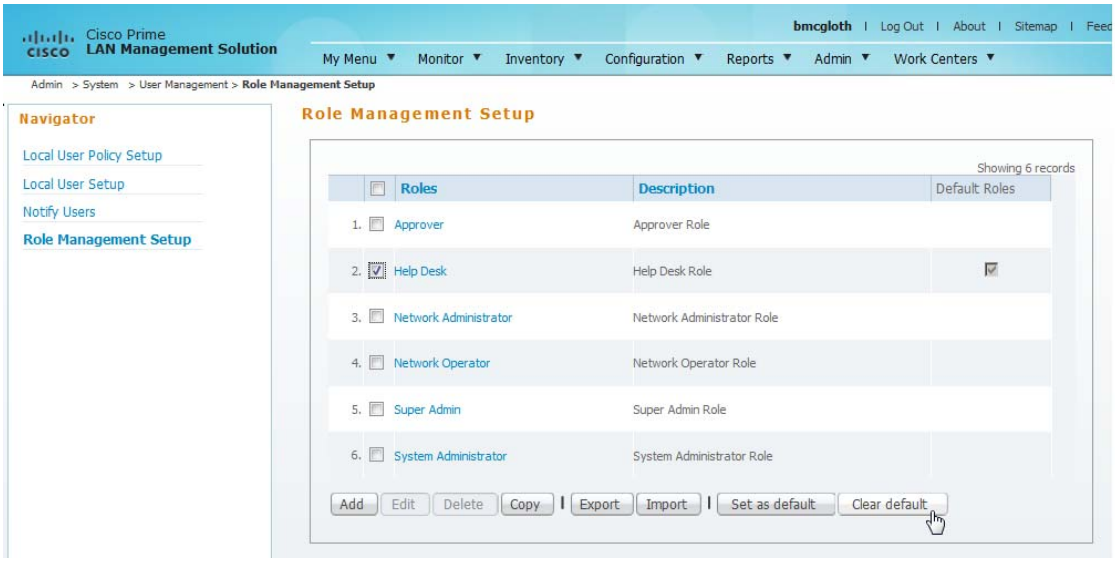
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
  - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
  - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. Requirements addressed include: Auditing.
  - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.

Sample Configuration

A centralized user database (Active Directory) is accessed by Cisco Secure ACS using TACACS+ services. Individual user IDs are assigned. Roles are defined within LMS and based on group membership. This configuration was used to address all of the safeguards listed under Access Control above.

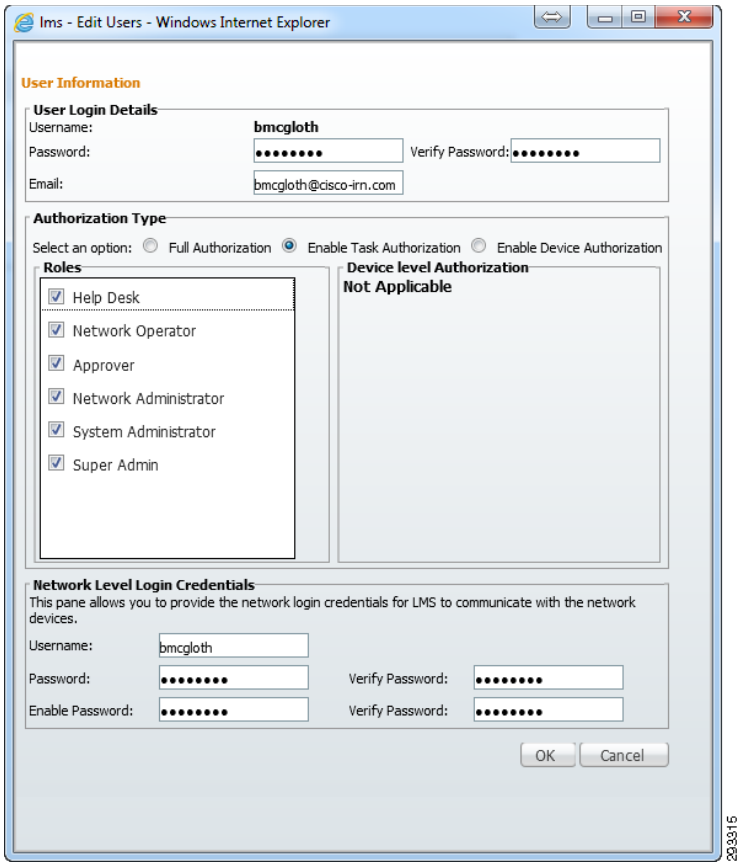
Cisco Prime LMS supports role-based user access. Users can be assigned to role groups and, based on privilege levels, have access to only the tasks they require for their job function. By default in Cisco Prime LMS, authenticated users are allowed help desk level access unless specifically configured and assigned to appropriate roles. To restrict access to only configured users, clear the default role option under Admin > System > User Management > Role Management Setup (see Figure 5-66).

Figure 5-66 Role Management Setup



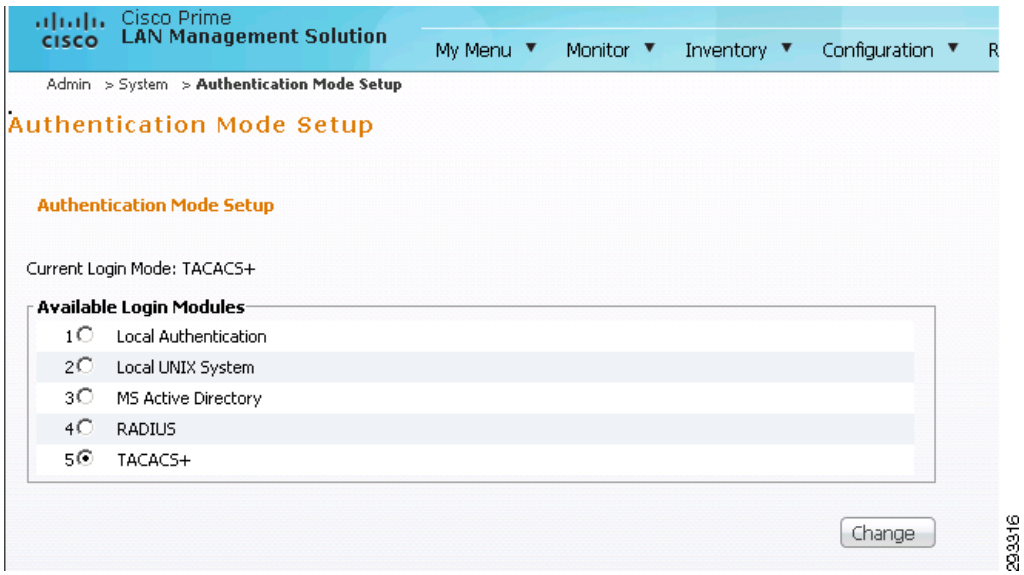
Local user accounts are configured to authorize role privileges and can also be used as fallback if the central authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration. (See Figure 5-67.)

Figure 5-67 LMS Local User Profile and Roles



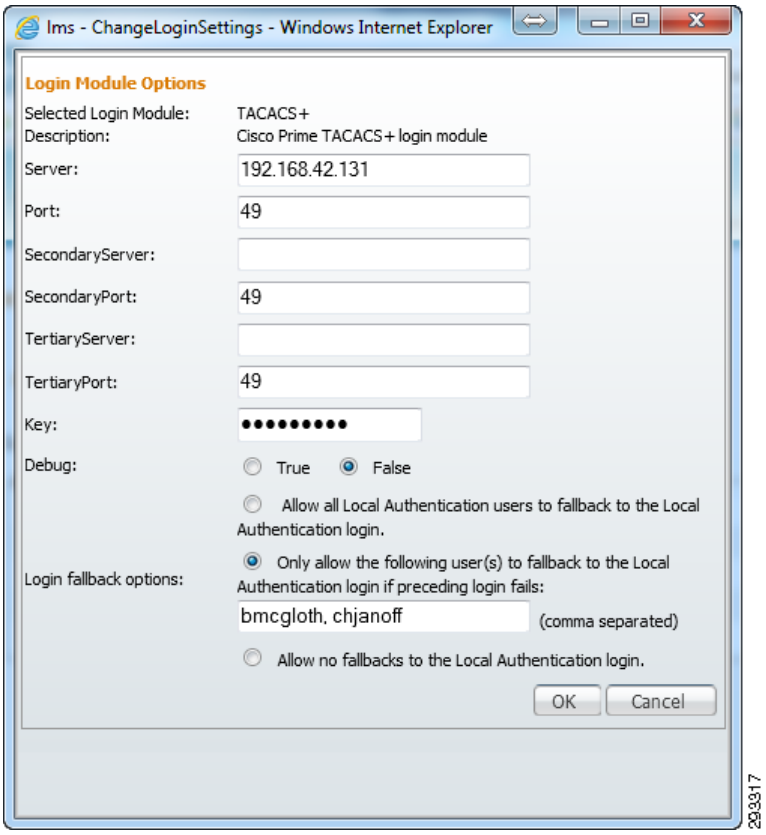
Several AAA services are available to externally authenticate users assigned to administer the system. Roles for these individuals are created and managed within the LMS system (see Figure 5-68). As of version 4, LMS no longer supports external authorization.

Figure 5-68 Authentication Mode Setup



In the TACACS server configuration, either all accounts or only specified accounts can be allowed for authentication in the event that the ACS server cannot be reached. (See Figure 5-69.)

Figure 5-69 Login Module Options

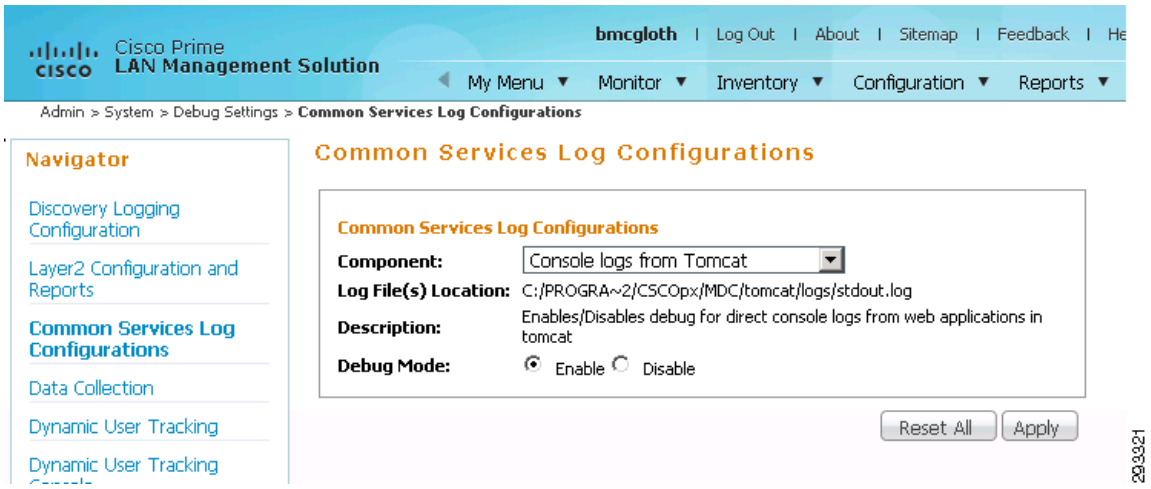


The majority of LMS system activities on the server are accomplished through jobs. Each of these jobs tracks the requestor, the success or failure, the type of event, and the systems against which they are executed. The Job Browser shows status of scheduled, current and past jobs. The jobs browser is located at Admin > Jobs > Browser.

To address the Incident Response and Auditing HIPAA Safeguards identified above, additional audit trail information for system configuration changes (for example, changing the authentication mode of the LMS Server from local to TACACS and back to local) require enabling debug mode logging for the Tomcat service. With debug mode enabled, the server is able to capture sufficient information for logging this configuration change and other similar system changes.

To enable debug mode for the Tomcat console, navigate to Admin > System > Debug Settings > Common Services Log Configurations (see Figure 5-70). Select “Console logs from Tomcat” in the component dropdown. Click the **Enable** radio button and then click **Apply**.

Figure 5-70 Common Services Log Configurations



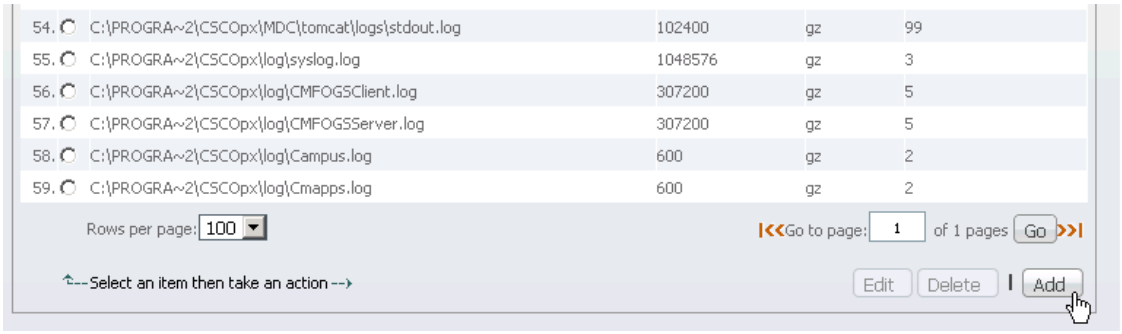
Note Enabling debugging may have a significant performance impact on the LMS system, depending on the number of users who are simultaneously accessing and managing the system. All web front end activity is logged in detail.

The "accesslogfilter.log" captures source IP address, date, time, and username for logged-in users as well as failed logins. Failed logins in this log have a "null" username. The attempted usernames of the failed logins appear in the Audit-Log-{date}.CSV report. These reports do not include the user's source IP address, so some manual correlation must be done between the two logs. These reports are generated at Reports > System Audit Reports > System, or available in \CSCOpx\MDC\log\audit. Information about currently logged-in users is available in Reports > System > Users > Who is logged On.

The "stdout.log" and "accesslogfilter.log" files should be added to the Log Rotation under Admin > System > Log Rotation.

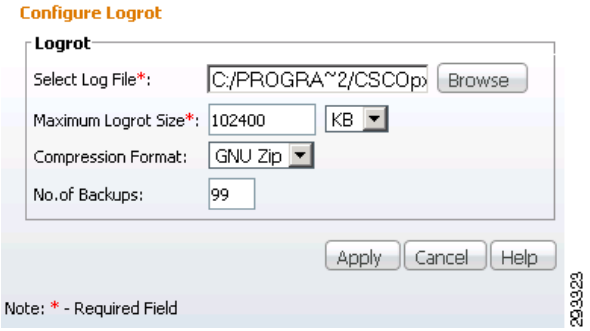
To add these logs to the rotation, click **Add** at the bottom of the page. (See Figure 5-71.)

Figure 5-71 Adding Logs to the Rotation



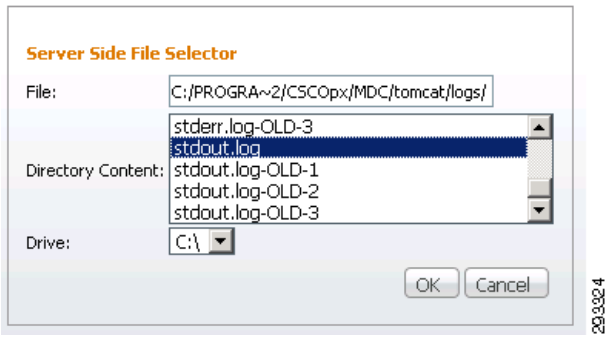
In the popup window, set the max file size needed to capture about a days' worth of information for your environment and usage. Set the number of backups to the maximum of 99. (See Figure 5-72.)

Figure 5-72 Configure Logrot



Click **Browse** and navigate to the file location as appropriate for the operating system; for example, C:/PROGRA~2/CSCOpx/MDC/tomcat/logs/stdout.log. (See Figure 0-8.)

Figure 5-73 Server Side File Selector



Click **OK** to complete the file section, and then **Apply** to complete the addition of the log rotation file.

The Cisco Prime LMS GUI and console scripts support periodic log rotation based on file size and can be configured for the maximum size of the file and number of files to maintain. A script must be created to copy these log files off the system to an external secure repository (for example, a directory on the RSA enVision server) because LMS is not natively capable of sending system events to a centralized repository or ensuring the integrity of the logs to the standards required. This script file should be automated and scheduled to run periodically at least daily (for example, every 1, 2, or 24 hours) via the operating system (Linux, Solaris, Windows) based on the deployment OS. Logs stored locally are buffered and require operator level privileges on the system to be viewed.

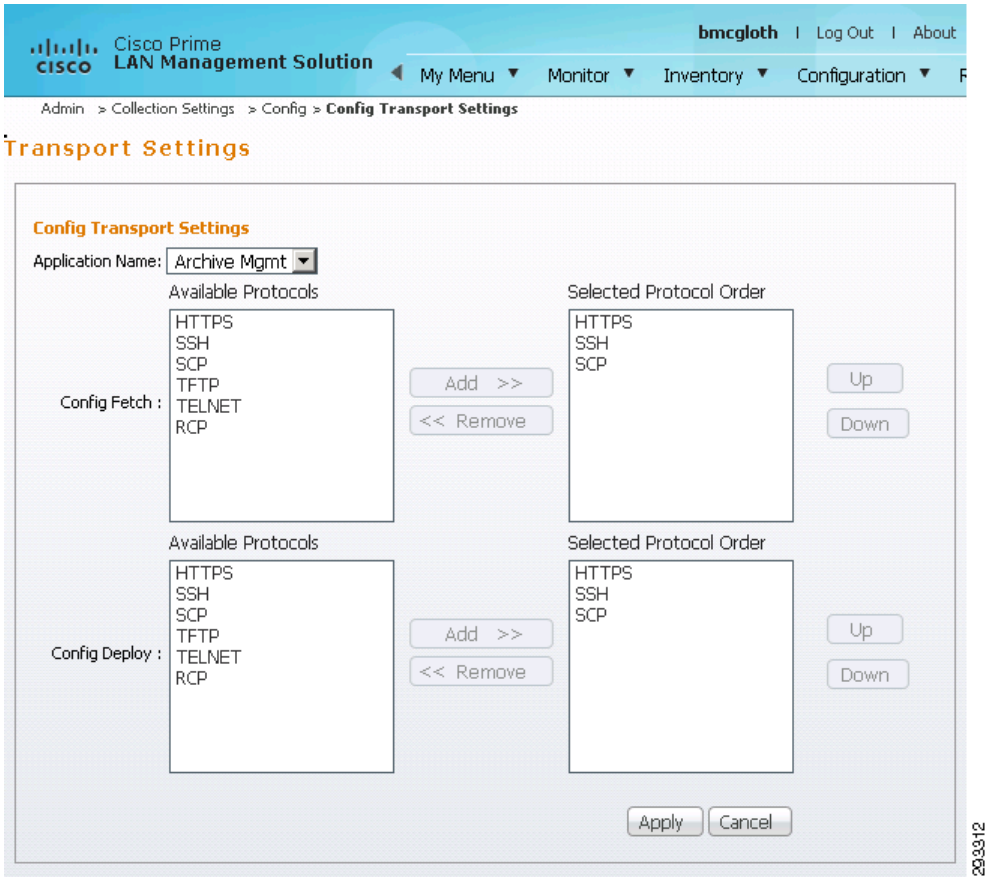
Logging enabled by implementing the following configuration statements in the CLI is only for system events such as software updates via the cars application utility:

```
logging 192.168.42.124
logging loglevel 6
```

RSA enVision supports the periodic collection of log files from Cisco LMS versions 3.2 and 4.0. The old method required the daily running of a .VBS script on the server (Windows only) where a file is created in the directory/files/rme/archive directory. It then required the installation of an RSA enVision NIC SFTP Agent, which is used to transfer the log files to the RSA enVision appliance. RSA recently added support for ODBC collection of change audit information from Cisco LMS. It is highly recommended to update to the latest RSA enVision ESU and move to this ODBC method as log collection occurs more frequently. ODBC importing was not validated for LMS at the time of this publication.

To secure authentication information and management of the LMS server and the devices that it manages, addressing Safeguard 164.308(a)(1)(i) Security Management, the LMS system was configured to support only encrypted protocols, as shown in Figure 5-74. Device management preferences are configured in Admin > Collection Settings > Config> Config Transport Settings. Add secure protocols to the list in order of preference and remove insecure protocols for each Application Named function.

Figure 5-74 Device Management Transport Settings



Cisco Prime LMS supports encrypted administrative access via SSH and HTTPS. SSH is enabled by default after installation. HTTPS can be enabled with a self-signed certificate or public certificate. To enforce the use of only SSL for the web interface of LMS, perform the following configurations, as shown in Figure 5-75. These configuration steps can also be found in the LMS 4.2 Administration Guide, page 53.

Figure 5-75 Enable Cisco Prime LMS Browser Security

To enable browser-server security, complete the following steps.

Procedure

Step 1 Select **Admin > Trust Management (4.2.2 patch) > Local Server > Browser-Server Security Mode Setup**.

The Browser-Server Security Mode Setup dialog box appears.

Step 2 Select the **Enable** option to enable SSL.

Step 3 Click **Apply**.

Step 4 Log out from your Cisco Prime session and close all browser sessions.

Step 5 Restart the Daemon Manager from the LMS Server CLI.

On Windows:

a. Enter `net stop crmdmgtd`

b. Enter `net start crmdmgtd`

On Solaris/Soft Appliance:

a. Enter `/etc/init.d/dmgtd stop`

b. Enter `/etc/init.d/dmgtd start`

Step 6 Restart the browser and the Cisco Prime session.

When accessing the LMS CLI, you need to enter the SHELL by using the **shell** command. Then you can execute the stop/start commands for the soft appliance.

If you have issues logging in to LMS (such as long delays), try disabling the launch of the LMS Getting Started page by default (as the first page after log in) by completing the following steps:

a. Open the properties file name “gs.properties” under the following path:

Windows:

```
/<<NMS-ROOT>>/MDC/tomcat/webapps/cwlms/WEB-INF/classes/com/Cisco/nm/gs/ui/gs.properties
```

Soft appliance:

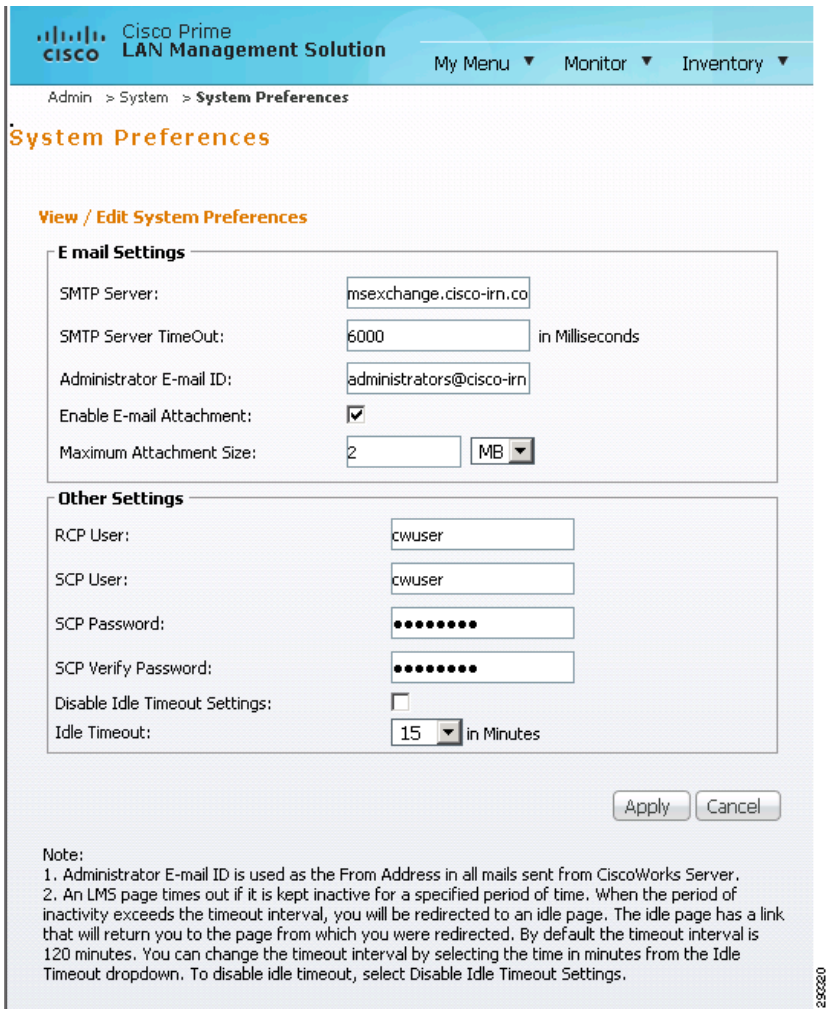
```
./opt/CSCOpx/MDC/tomcat/webapps/cwlms/WEB-INF/classes/com/cisco/nm/gs/ui/gs.properties
```

b. Update the field IS_DEFAULT_PAGE as “false”.

c. Clear the browser cache and login-in (Daemon restart not required).

HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of automatic logoff options. Cisco LMS supports session policies under the Admin > System > System Preferences tab. It is a best practice to change the session time-out to 15 minutes, as shown in Figure 5-76.

Figure 5-76 LMS System Preferences for Idle Timeout



As a best practice, NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. The Cisco Prime LMS appliance uses NTP to meet these requirements by implementing the following configuration statements:

```
ntp server 192.168.62.161 192.168.62.162
```

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Cisco Security Manager

The Cisco Security Manager is a powerful yet easy-to-use solution for configuring firewall, VPN, and IPS policies on Cisco security appliances, firewalls, routers, and switch modules.

Cisco Security Manager helps enable enterprises to manage and scale security operations efficiently and accurately. Its end-to-end tools provide consistent policy enforcement, quick troubleshooting of security events, and summarized reports from across the security deployment.

Cisco Security Manager enables you to centrally manage security policies over 250 types and models of Cisco security devices. Cisco Security Manager supports integrated provisioning of firewall, IPS, and VPN (most site-to-site, remote access, and SSL) services across the following:

- Cisco IOS/ISR/ASR routers
- Cisco Catalyst switches
- Cisco ASA and PIX security appliances
- Cisco Catalyst Service Modules related to firewall, VPN, and IPS
- Cisco IPS appliances and various service modules for routers and ASA devices

For a complete list of devices and OS versions supported by Cisco Security Manager, see *Supported Devices and Software Versions for Cisco Security Manager* at the following URL: http://www.cisco.com/en/US/products/ps6498/products_device_support_tables_list.html.

The high-performance and easy-to-use integrated event viewer allows you to centrally monitor events from IPS, ASA, and FWSM devices and correlate them to the related configuration policies. This helps identify problems and troubleshoot configurations. Then, using Configuration Manager, you can make adjustments to the configurations and deploy them. Event Viewer supports event management for Cisco ASA, IPS, and FWSM devices.

In addition to the Primary Event Data Store, events can be copied and stored in the Extended Event Data Store. The Extended Event Data Store can be used to back up and archive a larger number of events. This is useful for historical review and analysis of events where Event Viewer can gather event data from both the Primary Event Data Store and the Extended Event Data Store. The Extended Event Data Store can be enabled in Event Management in Security Manager's Administration settings.

For supported platforms and more information, see the “Monitoring and Diagnostics” section of the *User Guide for Cisco Security Manager 4.1* at the following URL: http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html.

The new integrated report management allows you to generate and schedule ASA, IPS, and remote access VPN reports. Reports for ASA and IPS devices are created by aggregating and summarizing events collected by the Event Viewer. Security reports can be used to efficiently monitor, track, and audit network use and security problems reported by managed devices. Report Manager helps in developing and customizing reports for Cisco ASA and IPS devices.

For supported platforms and more information, see the “Monitoring and Diagnostics” part of the *User Guide for Cisco Security Manager 4.1* at the following URL: http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html.

Table 5-15 PHI HIPAA Assessment Summary—Cisco Security Manager

Models Assessed	
Cisco Security Manager version 4.0.1	
HIPAA Safeguards Addressed	
Administrative	**Standards/Implementation Specifications**
164.308	(a)(1)(i) Security Management Process
	(a)(3)(ii)(A) Authorization/Supervision
	(a)(4)(ii)(B) Access Authorization
	(a)(4)(ii)(C) Access Establishment and Modification
	(a)(5)(ii)(C) Log-in Monitoring
	(a)(6)(i) Response and Reporting
Technical	**Standards/Implementation Specifications**
164.312	(a)((2)(i) Unique User Identification
	(b) Audit Controls
	(d) Person or entity authentication
HIPAA Standards Failed	
No HIPAA standards were failed.	
HIPAA Implementation Specifications Failed	
No HIPAA implementation specifications were failed.	

Primary PHI Function

The primary function of Cisco Security Manager is to implement security configuration in firewalls, routers, and intrusion detection devices based on policy templates to secure the ePHI data. The Cisco Security Manager allows for the secure configuration of network devices to enforce user access (authorization) to systems containing PHI. Additionally the Cisco Security Manager can run reports on access attempts and can help troubleshoot security events across the infrastructure allowing the organization to monitor access to systems and devices that contain ePHI.

Design Considerations

- Use descriptive notes for each rule set. These are displayed as remarks in the running configuration.
- Virtualize firewall rule set deployment by using a consistent interface naming standard.
- Apply the anti-spoofing feature to all interfaces using FlexConfig.

HIPAA Assessment Detail—HIPAA Safeguards Addressed

HIPAA safeguards are spread across multiple categories. The CSM allows healthcare-covered entities and business associates to meet access control safeguards in the Administrative and Technical categories. The access control can be applied to both internal and external users that access ePHI data.

All of the sample configurations of the CSM shown below were used to meet the following list of satisfied controls:

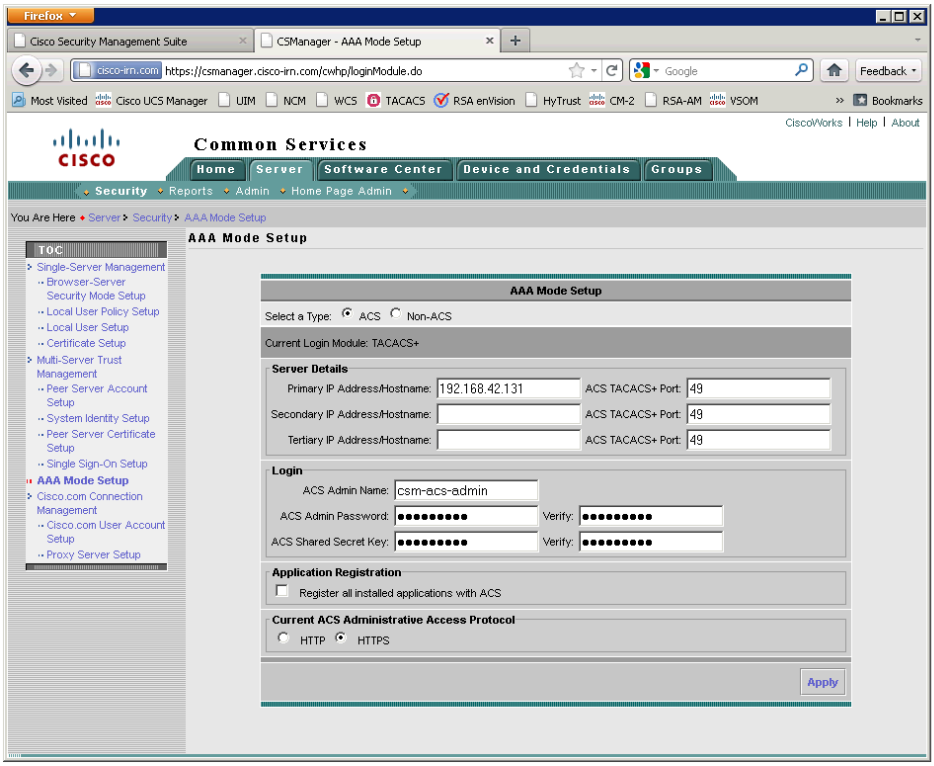
- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations it might be accessed. Requirements addressed include: Access Control and Auditing.
  - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
  - §164.308(a)(4)(ii)(C) Access Establishment and Modification. Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. Requirements addressed include: Access Control, Incident Response, and Auditing.
  - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
  - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
  - §164.312(a)(2)(i) Unique User Identification. Assign a unique name and/or number for identifying and tracking user identity. Requirements addressed include: Access Control and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
  - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. Requirements addressed include: Auditing.
  - §164.312(d) Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. Requirements addressed include: Access Control and Auditing.

Sample Configuration

Cisco CSM is designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership.

To secure authentication information and management of the CSM server, addressing Safeguard 164.308(a)(1)(i) Security Management, the CSM management console was configured to support HTTPS access only. Figure 5-77 shows that Cisco Security Manager is configured in Common Services so that only encrypted communications for administration are used, and AAA role setup type was implemented as Cisco Secure ACS and identified the appropriate Cisco Secure ACS servers.

Figure 5-77 CSM Secure Administration and AAA Policy



Sample Configuration

Cisco Security Manager is designed to track and monitor all administrative user access and events. To address the Incident Response and Auditing HIPAA safeguards identified above, Cisco Secure CSM can be configured to send its log data to the RSA enVision log management platform.

Figure 5-78, Figure 5-79, and Figure 5-80 show the Logs, Audit Report, and View Settings screens.

Figure 5-78 Logs

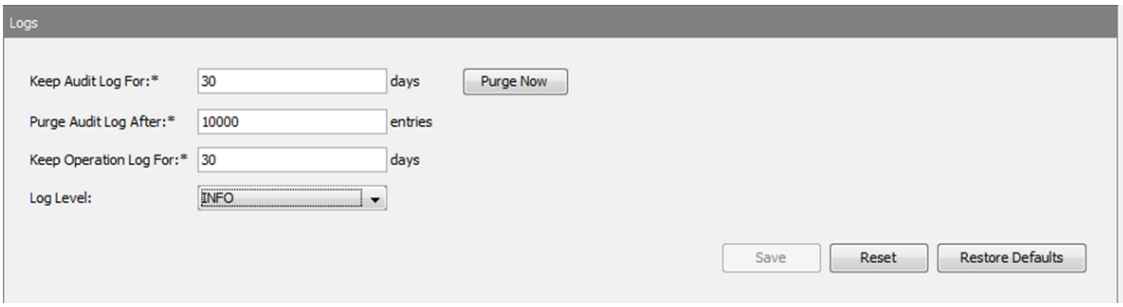


Figure 5-79 Audit Report

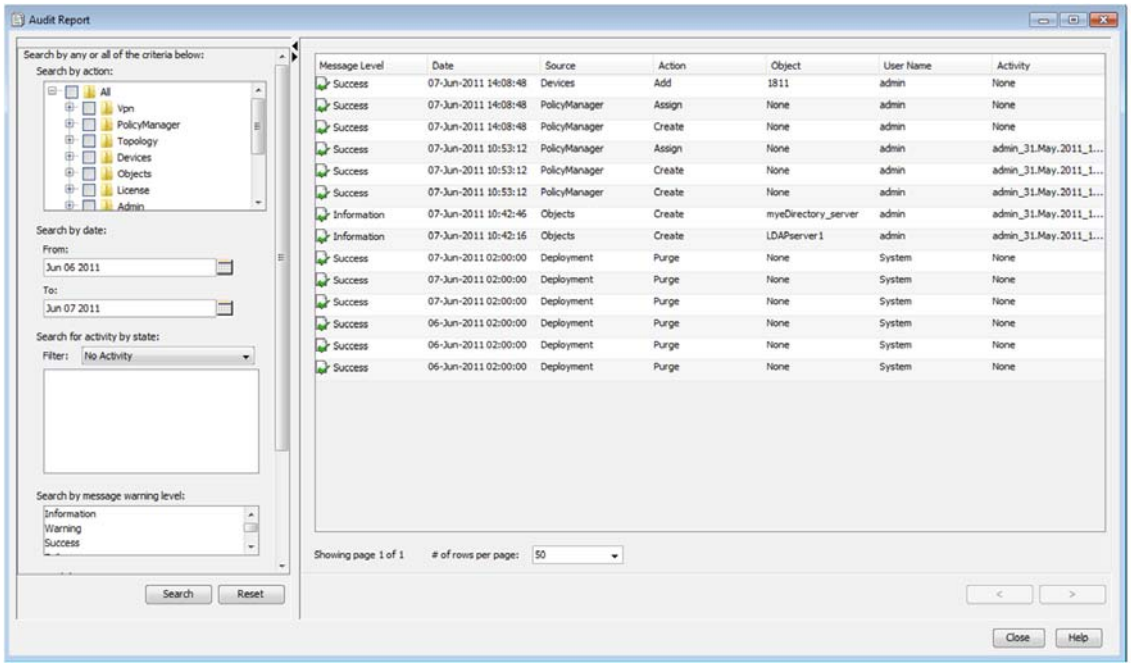
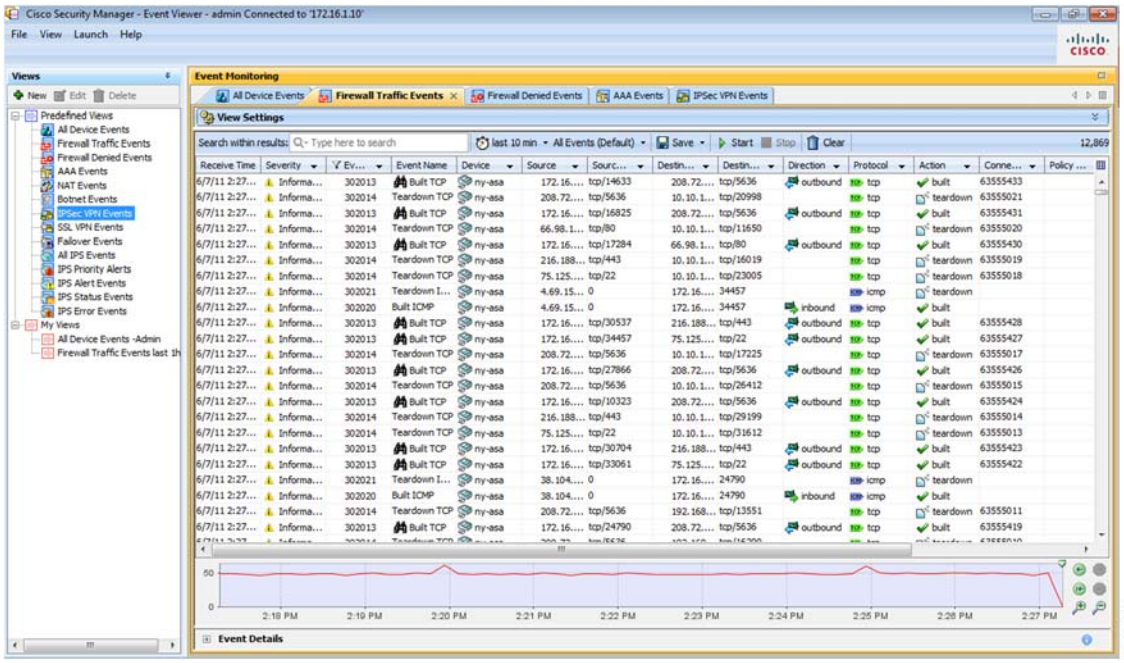
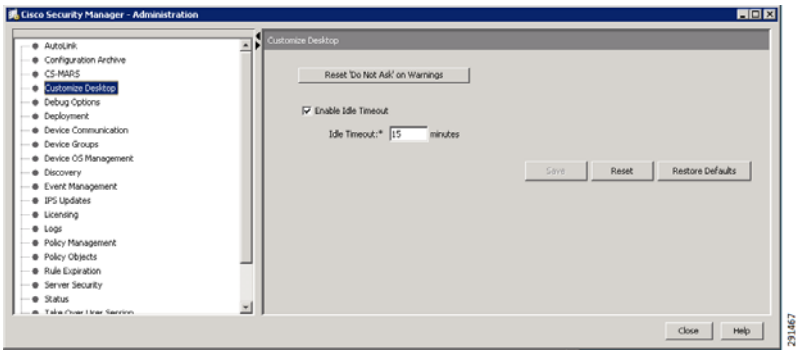


Figure 5-80 View Settings



HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of Automatic logoff options. Cisco CSM supports session idle timeout under the Administration Custom Desktop Settings tab. It is a best practice to change the session timeout to 15 minutes, as shown in Figure 5-81.

Figure 5-81 Customize Desktop



As a best practice, NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. Time synchronization for Windows servers is specified through the domain policy. Servers synchronize their clocks with the domain controller, which in turn is synchronized using NTP. This implementation of Cisco CSM was Windows-based.

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Encryption

RSA Data Protection Manager

RSA Data Protection Manager (formerly RSA Key Manager) provides encryption, tokenization, and key management capabilities. It can be used to achieve HIPAA requirements for protecting stored ePHI data, regardless of where the information resides.

RSA Data Protection Manager is an easy-to-use management tool for encrypting keys at the database, file server, and storage layers. It is designed to lower the total cost of ownership and simplify the deployment of encryption throughout the enterprise. It also helps properly secure information and enables its accessibility when needed at any point in its lifecycle through a powerful management console and built-in high availability features. RSA Data Protection Manager provides a comprehensive platform for enforcing and managing the security of sensitive data.

Table 5-16 PHI HIPAA Assessment Summary—Cisco RSA Data Protection Manager

Models Assessed	
RSA Data Protection Manager	version KM-3.1 / AM-6.1.SP3
HIPAA Safeguards Addressed	

Table 5-16 PHI HIPAA Assessment Summary—Cisco RSA Data Protection Manager

Administrative	Standards/Implementation Specifications
164.308	(a)(1)(i) Security Management Process
	(a)(3)(i) Authorization/Supervision
	(a)(4)(i) Access Authorization
	(a)(5)(i) Log-in Monitoring
	(a)(6)(i) Security Incident Procedures
Technical	**Standards/Implementation Specifications**
164.312	(a)(i) Access Control
	(b) Audit Controls
	(c)(1) Data Integrity
HIPAA Standards Failed	
No HIPAA standards were failed.	
HIPAA Implementation Specifications Failed	
No HIPAA implementation specifications were failed.	

Primary PHI Function

The primary function of RSA Data Protection Manager is to securely manage the keys that protect ePHI data.

This safeguard was met using the RSA Data Protection Manager to encrypt data in the database, file server, and storage. All ePHI data is encrypted to prevent unauthorized access or modification to the data. Unauthorized access attempts are logged and automatic notification can be sent to authorized personnel. With automated event notification, the RSA Data Protection Manager's detection capabilities can help an organization quickly identify and contain security violations.

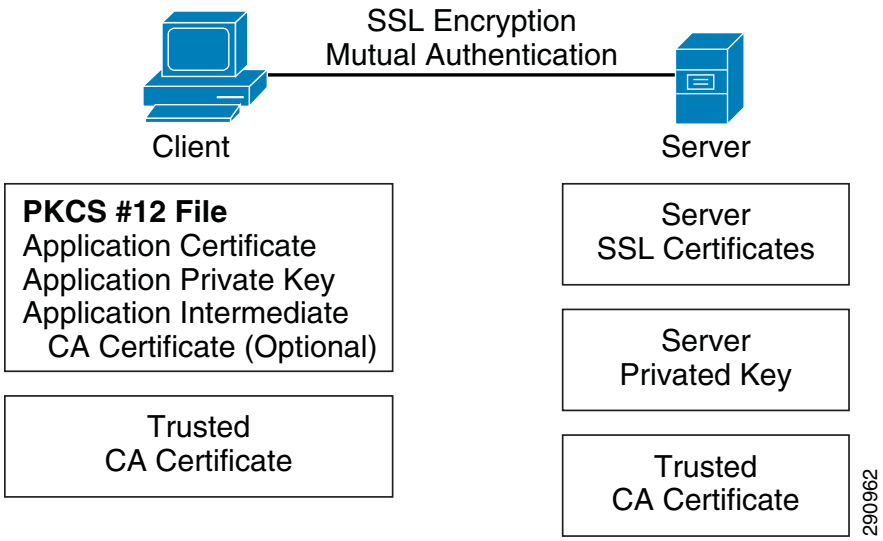
Design Considerations

RSA Data Protection Manager's encryption and key management capabilities can be used to store the data in a compliant manner. RSA Data Protection Manager provides application development libraries that support a wide range of development languages and enables developers to easily integrate encryption into point-of-sale, payment, CRM, ERP, and other business applications that create or process sensitive information. RSA Data Protection Manager can also be used to encrypt data as it flows to both disk and tape by providing key management services to Cisco MDS or EMC storage systems.

Because there were no PHI applications in the simulated lab environment, RSA Data Protection Manager was integrated with Cisco MDS to encrypt all data in the environment regardless of whether it was ePHI data or not.

In an RSA Data Protection Manager deployment, a PKI needs to be set up to enable secure communication between the RSA Data Protection server and its clients. (See Figure 5-82.)

Figure 5-82 RSA Data Protection Manager Deployment



The certificates and credentials that need to be prepared include:

- Client PKCS#12 certificate and key pair—Used to authenticate RSA Data Protection Manager clients to the RSA Data Protection Server
- Server SSL certificate and key pair—Used by RSA Data Protection Manager Clients to authenticate the server
- Trusted CA certificate—Installed on both clients and the server to verify the signature of certificates sent by a peer. For example, a RSA Key Manager Client has a trusted CA certificate to verify the signature of the server certificate.
- Middle CA certificate (optional)—If a certificate is not signed directly by a trusted CA certificate, a middle CA certificate should be installed and sent during SSL connection to verify the certificate chain.

Because of vulnerabilities with RSA signatures with a small public exponent, especially 3, RSA recommends that an exponent of F4 (216+1) be used.

HIPAA Assessment Detail—HIPAA Safeguards Addressed

All of the sample configurations of RSA Data Protection Manager shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
  - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.

  - §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
  - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
  - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. Requirements addressed include: Auditing.
  - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
- Integrity—Protect electronic protected health information from improper alteration or destruction as required by HIPAA Technical Safeguards.
  - §164.312(c)(1) Data Integrity. Implement policies and procedures to protect health information from improper alteration or destruction.

Sample Configuration

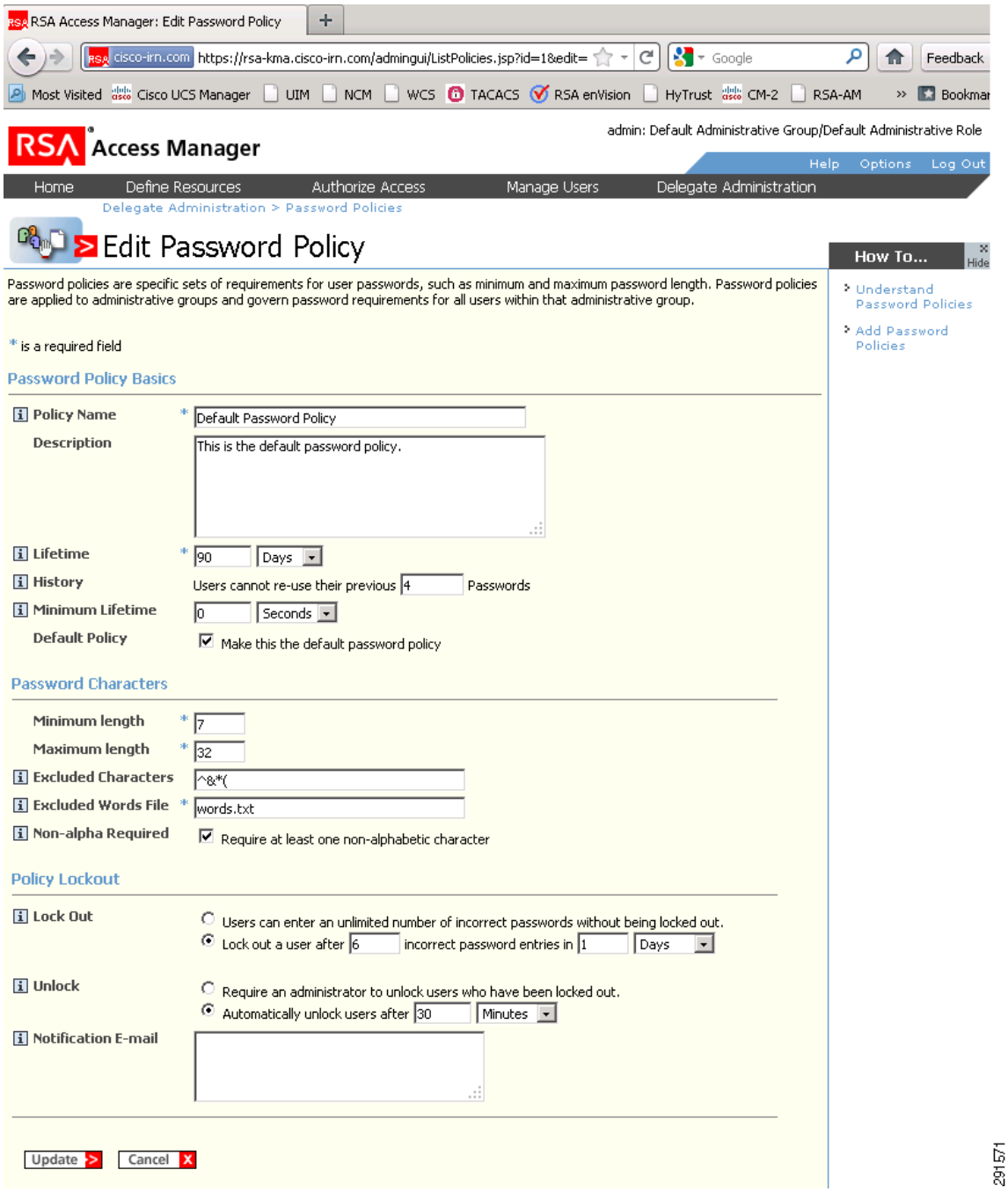
RSA Data Protection Manager embeds and is protected by RSA Access Manager, which has very powerful and flexible capabilities to define password and account lockout policies and is designed to meet all of the Access Control safeguards above. The included RSA Access Manager Internal Database is used. Within RSA Data Protection Manager (and the included Access Manager), individual user IDs are assigned. Roles are defined and based on group membership.

RSA Data Protection Manager embeds and is protected by RSA Access Manager, which has very powerful and flexible capabilities to define password and account lockout policies that can meet all of the above criteria.

Configuration of user policies is performed via the administration console that can be accessed at the following URL: https://<server address>/admingui/Login.jsp.

Figure 5-83 shows an appropriate password policy for compliance.

Figure 5-83 Password Policy Settings



RSA Data Protection Manager is designed to track and monitor all administrative user access and events. RSA Data Protection Manager can be configured to send its log data to the RSA enVision log management platform to address the Incident Response and Auditing HIPAA Safeguards identified above. The configuration procedure is documented in the enVision Event Source Configuration Guide for RSA Data Protection Manager, which can be found at RSA Secure Care Online (https://knowledge.rsasecurity.com/).

NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. The appliance uses NTP to meet these requirements by specifying the appropriate NTP servers during the installation steps. If NTP servers need to be modified, use the following steps:

1. Open the /etc/ntp.conf file.
2. Under the List Servers section, provide the ntp server ip address or host name to the server parameter.
3. Save the /etc/ntp.conf file.
4. Execute the following commands (as root) to forcibly synchronize the clock of the appliance to the NTP server:

a. Stop the NTPD daemon by typing the following:

```
service ntpd stop
```

b. Execute the following command at least three times (to minimize the offset):

```
ntpdate -u <ntpserver>
```

c. Start the NTPD daemon by typing the following:

```
service ntpd start
```

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Storage

EMC SAN Disk Array

The EMC SAN disk array is used to securely store sensitive compliance data within the data center. Using virtual storage technology, organizations are able to safely combine (in-scope) sensitive date with (out-of-scope) data while maintaining the compliance boundary.

EMC technology combines midrange networked storage with innovative technology and robust software capabilities to manage and consolidate your data.

Table 5-17 PHI HIPAA Assessment Summary—EMC SAN Disk Array

Models Assessed	
EMC CLARiiON CX-240	
EMC Unified Infrastructure Manager version 2.0.1.1.160	
HIPAA Safeguards Addressed	
Administrative	**Standards/Implementation Specifications**
164.308	(a)(1)(i) Security Management Process
	(a)(3)(ii)(A) Authorization/Supervision
	(a)(4)(ii)(B) Access Authorization
	(a)(5)(ii)(C) Log-in Monitoring
	(a)(6)(ii) Response and Reporting
Technical	**Standards/Implementation Specifications**
164.312	(a)(i) Unique User Identification
	(b) Audit Controls
	(c)(1) Data Integrity
HIPAA Standards Failed	
No HIPAA standards were failed.	
HIPAA Implementation Specifications Failed	
No HIPAA implementation specifications were failed.	

Primary PHI Function

The primary function of the EMC SAN disk array is to store ePHI data. There is no direct PHI requirement for this storage function. This control was met using the EMC SAN Disk Array granular access control to minimize the access to the ePHI data in storage. Additionally the EMC SAN Disk Array can work with application security controls to minimize access privileges to ePHI data. This helps meet the requirement for minimal use by allowing the individual to only access what is needed to perform the job function. Users can be assigned to groups and, based on privilege levels, have access to only the information they require for their job function.

Design Considerations

The EMC SAN disk array is a primary component of VCE Vblock architecture. Vblock 1 is designed for medium-to-high numbers of virtual machines, and is ideally suited to a broad range of usage scenarios, including shared services, e-mail, file and print, virtual desktops, and collaboration.

HIPAA Assessment Detail—HIPAA Safeguards Addressed

HIPAA safeguards are spread across multiple categories. The EMC SAN allows healthcare covered entities and business associates to meet access control safeguards in the Administrative and Technical categories. The access control can be applied to both internal and external users that access ePHI data.

All of the sample configurations of the EMC SAN Disk Array shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations it might be accessed. Requirements addressed include: Access Control and Auditing.
  - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
  - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
  - §164.312(a)(2)(i) Unique User Identification. Assign a unique name and/or number for identifying and tracking user identity. Requirements addressed include: Access Control and Auditing.
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
  - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
  - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. Requirements addressed include: Auditing.
- Integrity—Protect electronic protected health information from improper alteration or destruction as required by HIPAA Technical safeguards.
  - §164.312(c)(1) Data Integrity. Implement policies and procedures to protect ePHI from improper alteration or destruction. Requirements addressed include: Encryption, Integrity, and Auditing.

Sample Configuration

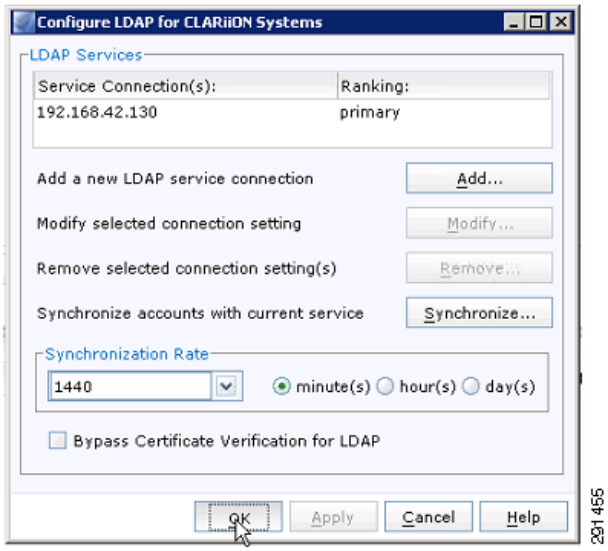
EMC SAN Disk Array is designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. A centralized user database (Active Directory) is accessed by the EMC SAN Disk Array using LDAP services. Individual user IDs are assigned. Roles are defined and based on group membership

When you start a session, Unisphere prompts you for a username, password, and scope (local, global, or LDAP). These credentials are encrypted and sent to the storage management server. The storage management server then attempts to find a match within the user account information. If a match is found, you are identified as an authenticated user.

Step 1 To configure LDAP authentication, go to the Domains tab, then select **Configure LDAP for CLARiiON Systems** from the Users menu on the left.

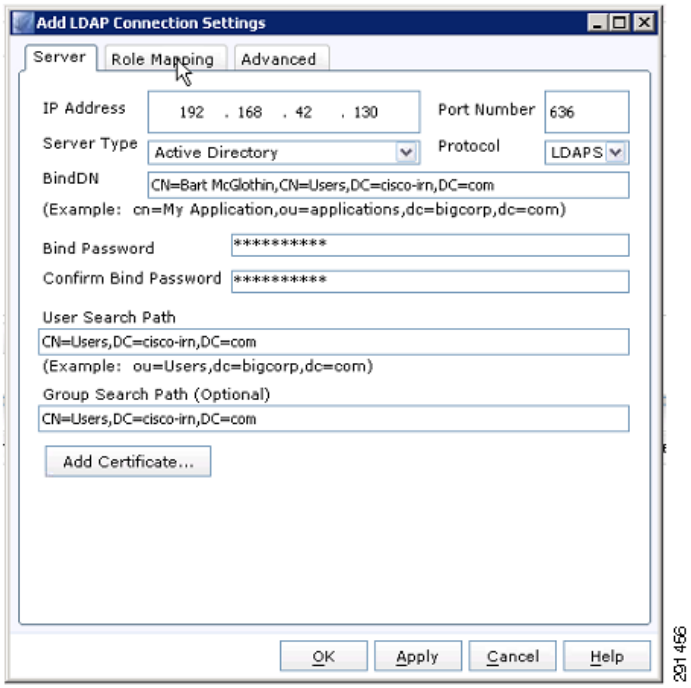
Step 2 Add a new LDAP service by clicking **Add** and then **OK**, as shown in Figure 5-84.

Figure 5-84 Adding LDAP Service



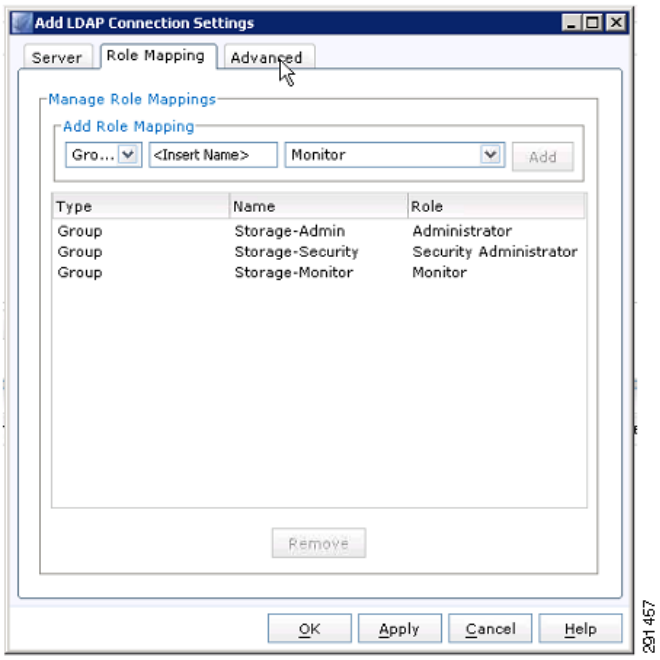
Step 3 Configure the LDAP server for Active Directory, as shown in Figure 5-85.

Figure 5-85 Configuring the LDAP Server for Active Directory



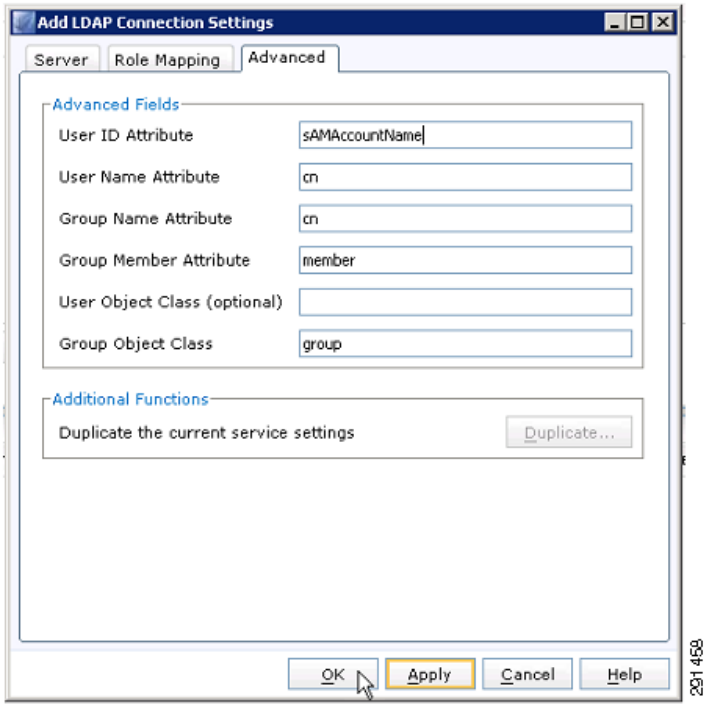
Step 4 After communications are established with the LDAP service, specific LDAP users or groups must be given access to Unisphere by mapping them to Unisphere roles. The LDAP service merely performs the authentication. Once authenticated, user authorization is determined by the assigned Unisphere role. The most flexible configuration is to create LDAP groups that correspond to Unisphere roles. This allows you to control access to Unisphere by managing the members of the LDAP groups. Roles were configured as shown in Figure 5-86.

Figure 5-86 Role Mapping



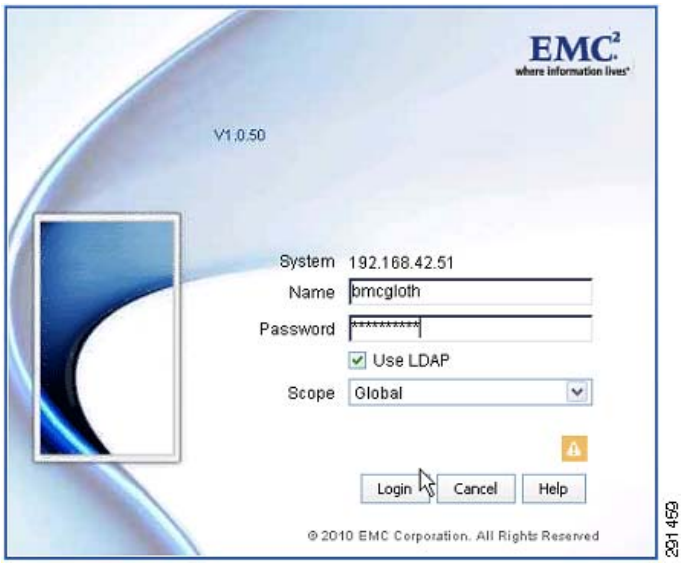
Step 5 The Advanced features were left at their default settings, as shown in Figure 5-87.

Figure 5-87 Advanced Settings



Step 6 You can then log out, and log back in, selecting the **Use LDAP** option for centralized authentication, as shown in Figure 5-88.

Figure 5-88 Selecting Use LDAP Function



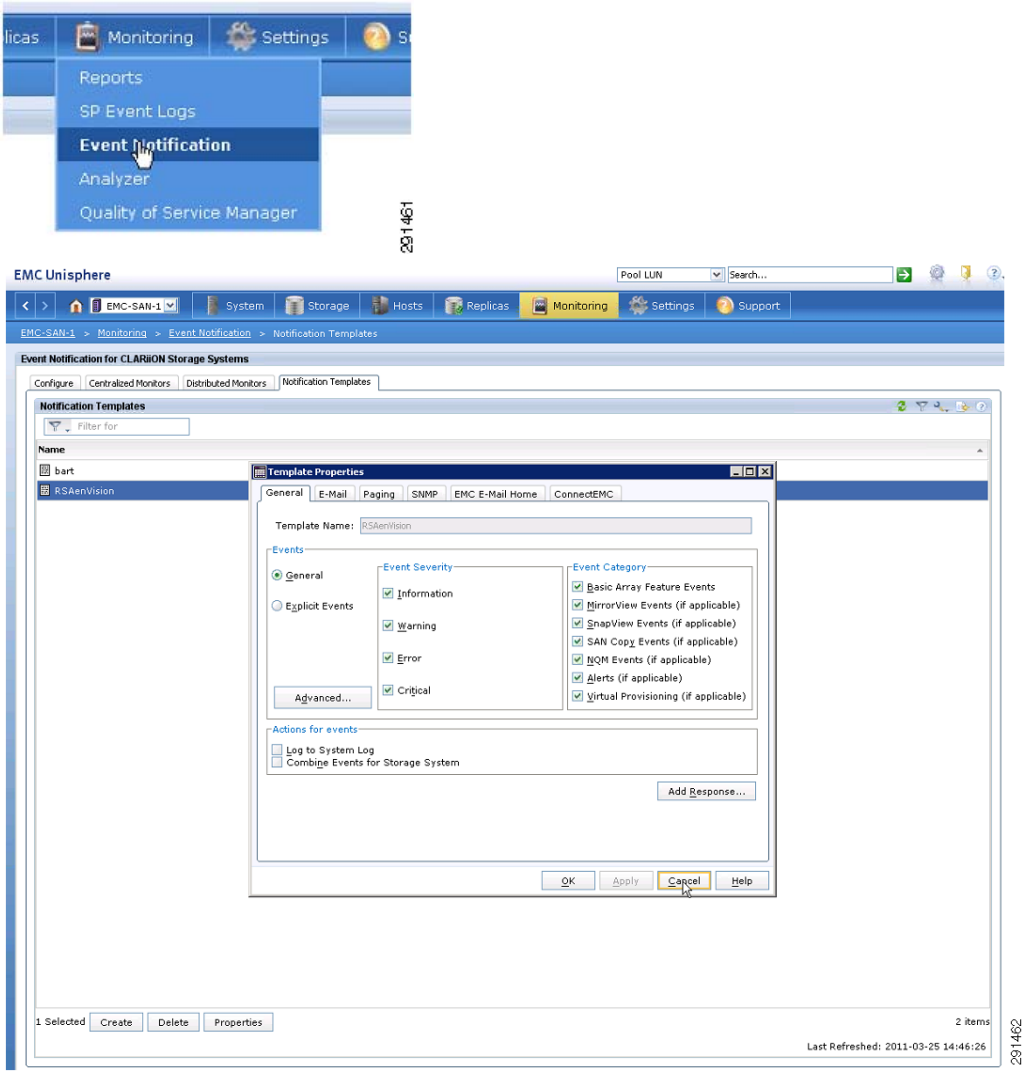
Step 7 For further installation information, see the *FLARE 30 Security Configuration Guide* on EMC Powerlink for configuring LDAP/Active Directory authentication.

EMC CLARiiON is designed to track and monitor all administrative user access and events.

To address the Incident Response and Auditing HIPAA safeguards identified above, SP event logs on CLARiiON storage systems can store only a fixed number of events, and wrap if that limit is exceeded. This may take days, weeks, months, or years depending on the logging activity. To keep all logs for a set period of time, you need to archive the logs from the CLARiiON storage system on a regular basis. You can do this with the CLI **getlog** command, but a much more integrated method is to use the "log to system log" option of the Event Monitor template to log events to the Windows system log. You can then archive these logs as required.

Additional SNMP Traps are configured to send event notifications directly and immediately to RSA enVision. (See Figure 5-89.)

Figure 5-89 Using Log to System Log Option

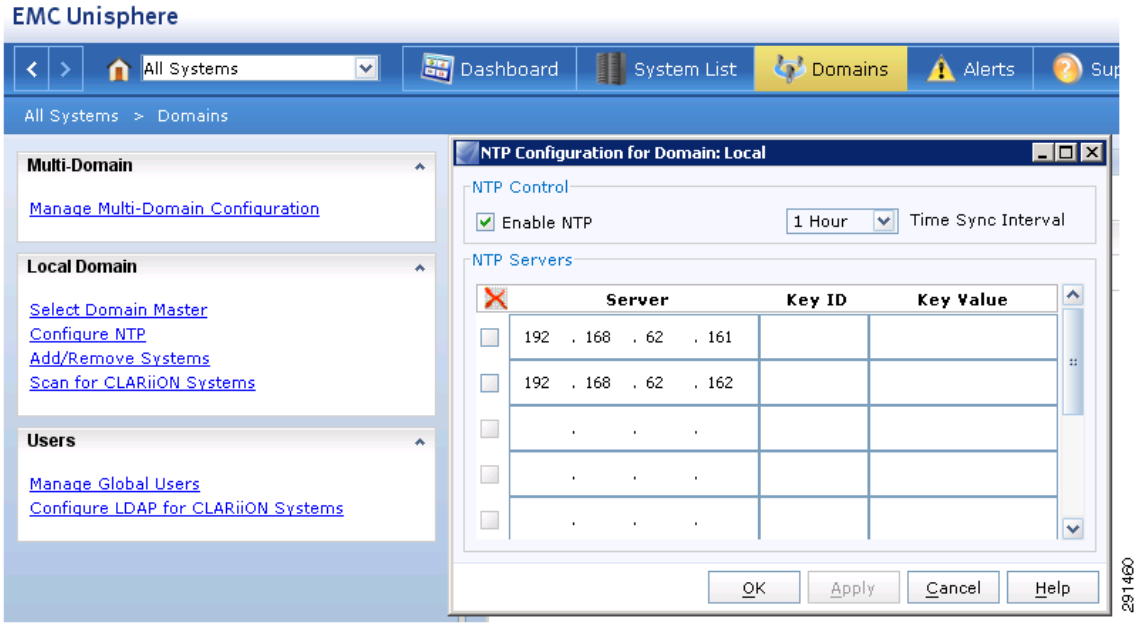


To secure authentication and management of the EMC Array, addressing Safeguard 164.308(a)(1)(i) Security Management, when you connect to Unisphere through http://<clariion_ip> (port 80), a Java applet is delivered to the browser on your computer. The applet establishes a secure connection over SSL/TLS (port 443) with the storage management server on the CLARiiON storage system. Therefore, even though “https://” is not displayed in the browser, the connection is secure.

As a best practice, NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. EMC CLARiiON uses Network Time Protocol (NTP) to update and synchronize local clock facilities.

CLARiion uses the NTP configuration statements shown in Figure 5-90.

Figure 5-90 NTP Configuration for Domain: Local



Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Monitoring

RSA enVision

RSA enVision is a security information and event management (SIEM) platform that addresses HIPAA safeguards to track and monitor all access to systems and network resources containing ePHI data. RSA enVision does this by collecting, permanently archiving, and processing all the log and event data generated by devices and applications within your network, and generating alerts when it observes suspicious patterns of behavior. Administrators can interrogate the full volume of stored data through an intuitive dashboard, and can use advanced analytical software to gain visibility and understanding of how their network is used and the threats and risks to the infrastructure and applications.

The RSA enVision platform can draw logs from tens of thousands of devices at once, including Cisco network devices, the VCE Vblock infrastructure, the VMware virtual environment, Cisco ASA firewalls, Cisco IPS devices, Cisco IronPort E-mail Appliance, other RSA products, and the HyTrust appliance. Out of the box, RSA enVision can produce compliance reports and alerts based on the log and event data it collects. RSA enVision also offers powerful tools to create custom reports and alerts specific to your environment.

Table 5-18 PHI HIPAA Assessment Summary—RSA enVision

Models Assessed	
RSA enVision version 4.0, Revision 5	
HIPAA Safeguards Addressed	
Administrative	**Standards/Implementation Specifications**
164.308	(a)(1)(i) Security Management Process
	(a)(1)(ii)(D) Information System Activity Review
	(a)(3)(i) Authorization/Supervision
	(a)(5)(i) Log-in Monitoring
	(a)(6)(i) Security Incident Procedures
	(a)(6)(ii) Response and Reporting
Technical	**Standards/Implementation Specifications**
164.312	(b) Audit Controls
HIPAA Standards Failed	
No HIPAA standards were failed.	
HIPAA Implementation Specifications Failed	
No HIPAA implementation specifications were failed.	

Primary PHI Function

The primary function of RSA enVision is to securely store and correlate the system logs that is receives.

Design Considerations

Depending on the size of your network, RSA enVision may be deployed as a standalone, self-contained, security-hardened appliance or in a distributed deployment to cope with the demands of the largest enterprise networks. When deployed in a distributed architecture, multiple dedicated appliances are deployed where required to perform key roles. Local and remote collectors perform data collection. Data servers manage the data. Application servers perform analysis and reporting. Data itself can be stored using direct attached, online, near-line or offline storage from the full EMC storage portfolio.

RSA enVision does not require any client-side agents to pull log or event data from your infrastructure or applications. RSA enVision can integrate with event sources through standard protocols such as syslog or SNMP by configuring the event source to send data to enVision. For richer event data, enVision integrates with some event sources through their APIs or directly with their database backends. Specific event source device configuration procedures can be found at RSA Secure Care Online (https://knowledge.rsasecurity.com/)

RSA enVision is sold as a standalone appliance. It is available in a variety of hardware options based on the requirements of the enterprise design. The system comes pre-installed on an already hardened operation system.

HIPAA Assessment Detail—HIPAA Safeguards Addressed

All of the sample configurations of the RSA enVision shown below were used to meet the following list of satisfied controls:

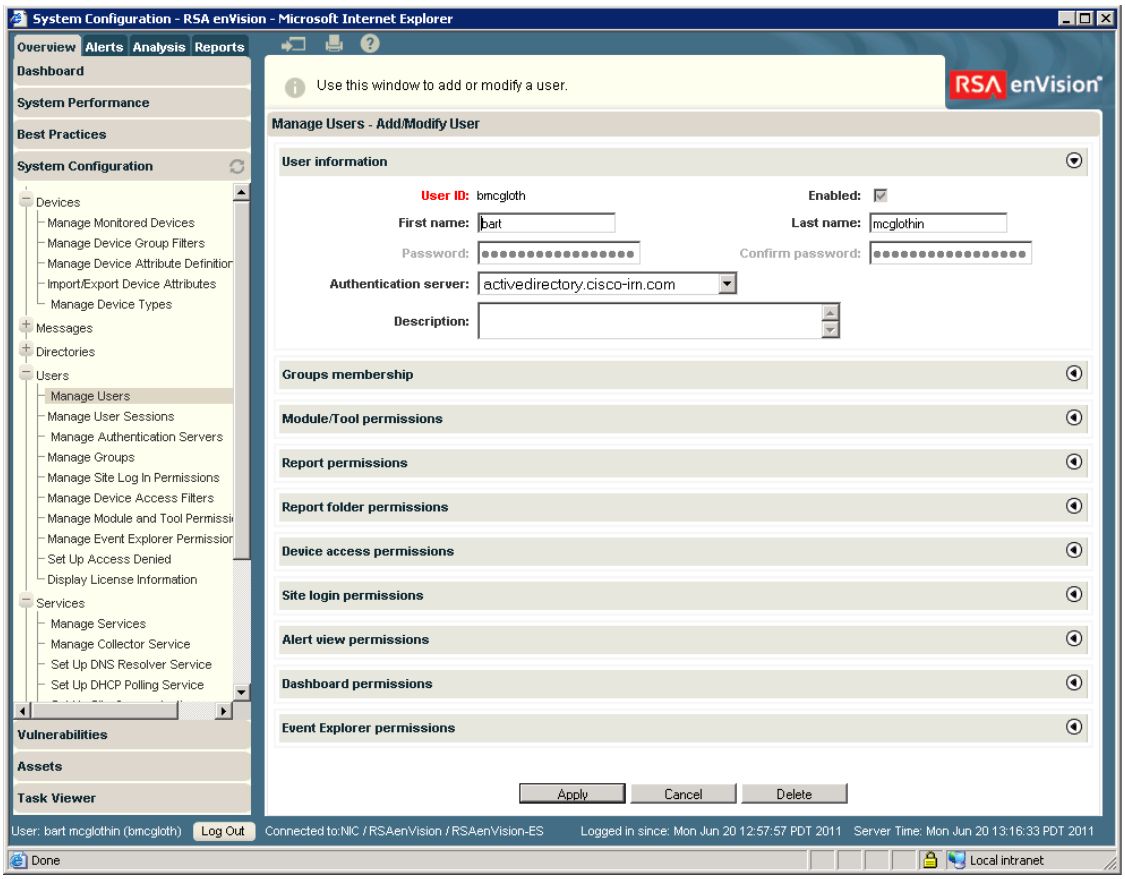
- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.308(a)(1)(ii)(D)Information System Activity Review. Implement procedures to regularly review records of information system activity, such as audit logs, access reports and security incident tracking.
  - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
  - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
  - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. Requirements addressed include: Auditing.
  - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.

Sample Configuration

The RSA enVision Internal Database is used (as part of its local Windows Active Directory). For validation, RSA enVision was linked to the centralized user database (Active Directory) using LDAP. Within RSA enVision, individual user IDs are assigned. Roles are defined and based on group membership.

RSA enVision management interfaces implement role-based access control that can be used to restrict access to privileged user IDs, as shown in Figure 5-91.

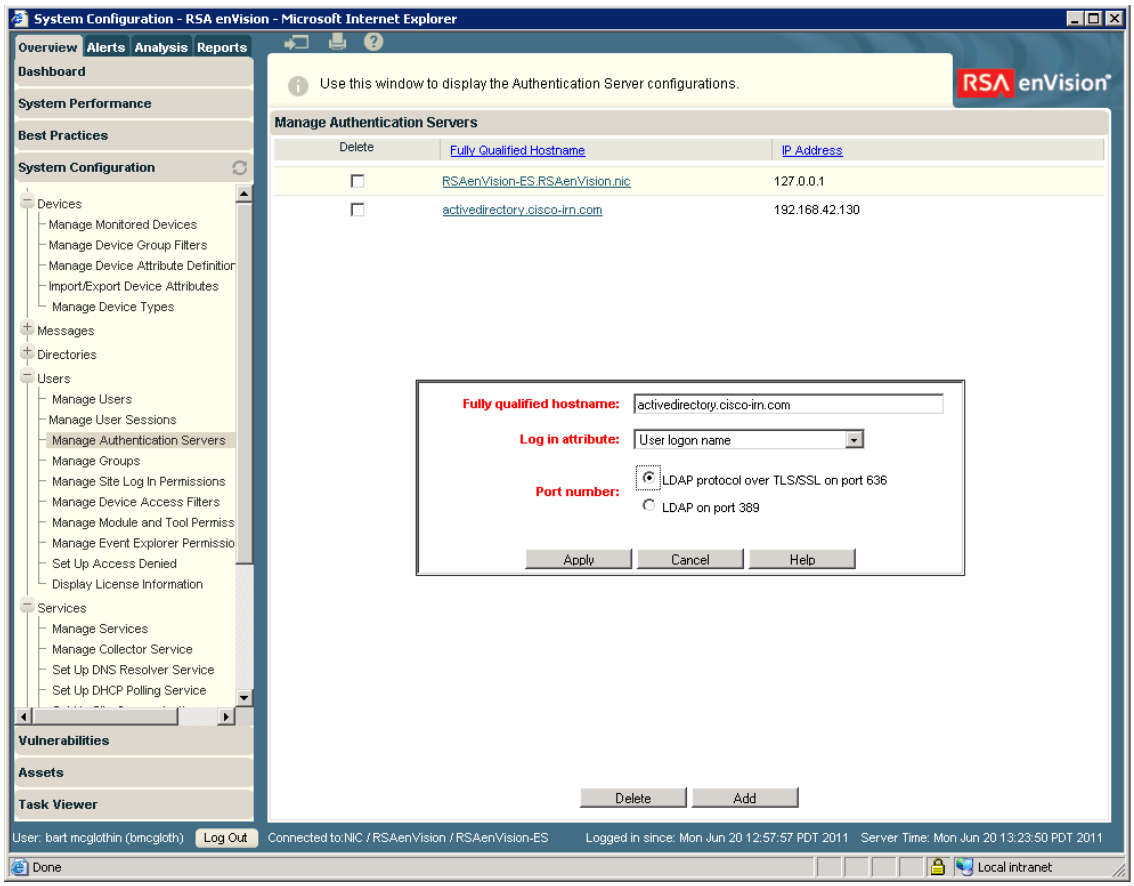
Figure 5-91 RSA enVision User Profile



RSA enVision's access control system defaults to deny access.

RSA enVision is configurable to use its local Active Directory database, or an external database via LDAP, as shown in Figure 5-92.

Figure 5-92 RSA enVision Authentication Servers



RSA enVision is designed to track and monitor all administrative user access and events. To address the Incident Response and Auditing HIPAA safeguards identified above, it performs the role of a central logging repository. RSA enVision collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

RSA enVision delivers mirrored, unfiltered data to its Internet Protocol Database, which provides the ability to retain data in its original format. Further, “write once, read many” capabilities help ensure that the mirrored copy remains intact, even if the original data is compromised. RSA enVision-captured event logs are stored on a hardened operating system and protected using an integrity check mechanism.

To secure authentication information and management of the RSA enVision server, addressing Safeguard 164.308(a)(1)(i) Security Management, the management console is accessible only via HTTPS.

As a best practice, NTP is used to synchronize clocks among network devices. Time synchronization for this windows server is specified through the Domain Policy because the RSA enVision appliance is itself a Domain Controller. The server synchronizes its clock to know time sources using NTP as specified in the initial appliance setup. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

HyTrust Appliance

Vblock Infrastructure Platforms from VCE allow organizations to take advantage of the architectural, operational, and financial benefits of virtualization in their PHI infrastructure. HyTrust Appliance (HTA) complements Vblock capabilities by providing:

- Access control for virtual infrastructure including least privilege, separation of duties, and two-factor authentication
- Granular and exhaustive logging and auditing
- Segmentation of infrastructure to support virtualized applications

Virtualized technologies create additional security requirements to ensure that the virtualized environment security controls are appropriate for the data sensitivity. This requirement is consistent with additional risks introduced by mobility and the fast-paced change rate of virtualized assets that can now be reconfigured, relocated, and duplicated by remote administrators. These capabilities combined with poor access control create a significant risk. Hypervisor logs geared toward software maintenance and troubleshooting are obviously useful, but not in the context of a compliance audit.

HyTrust Appliance systematically addresses the three broad areas of IT control objectives (access and user administration, change and configuration, and operations), by proactively enforcing policies for all administrative access, regardless of access method: Secure Shell (SSH) to host, VMware vSphere client to host, or VMware vCenter or any of the programmatic access. HyTrust Appliance provides two-factor authentication and role-based access control, logical segmentation of shared infrastructure, root password vaulting, and audit-quality logs of every attempted access.

Table 5-19 PHI HIPAA Assessment Summary—HyTrust Appliance

Models Assessed	
HyTrust version 2.2.1.14064	
HIPAA Safeguards Addressed	
Administrative	**Standards/Implementation Specifications**
164.308	(a)(1)(i) Security Management Process
	(a)(3)(ii)(A) Authorization/Supervision
	(a)(4)(ii)(B) Access Authorization
	(a)(5)(ii)(C) Log-in Monitoring
	(a)(6)(ii) Response and Reporting
Technical	**Standards/Implementation Specifications**
164.312	(a)(1) Access Control
	(b) Audit Controls
HIPAA Standards Failed	
No HIPAA standards were failed.	

Table 5-19 PHI HIPAA Assessment Summary—HyTrust Appliance

HIPAA Implementation Specifications Failed
No HIPAA implementation specifications were failed.

Primary PHI Function

The primary function of HyTrust Appliance is to provide an automated control and audit facility for the virtual infrastructure and cloud stack.

Design Considerations

Define rules and deploy policy to activate protection for the virtual infrastructure.

Administrators can define custom rules that restrict entitlement based on specific virtual infrastructure objects that users need to access and manage. Rules that define entitlement can be based on pre-defined roles or administrators can use custom user-defined roles.

The HyTrust appliance provides complete logging of administrator actions by proxying VMware vCenter client connections to the vSphere management server, and clients that try to connect directly to ESX/ESXi hosts. This logging includes the source IP address of the clients, permitted actions and actions that are blocked because the client may not have sufficient privileges.

HIPAA Assessment Detail—HIPAA Safeguards Passed

The HyTrust Appliance allows for management of user access (authorization) to systems containing ePHI. Additionally, the HyTrust Appliance can prevent unauthorized devices from accessing systems containing ePHI and protect access from unauthorized locations.

The HyTrust Appliance logs can be used to identify unauthorized attempts to connect to systems containing PHI to help meet the supervision requirements.

All of the sample configurations of the HyTrust Appliance shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
  - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
  - §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.

  - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.

- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
  - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
  - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. Requirements addressed include: Auditing.

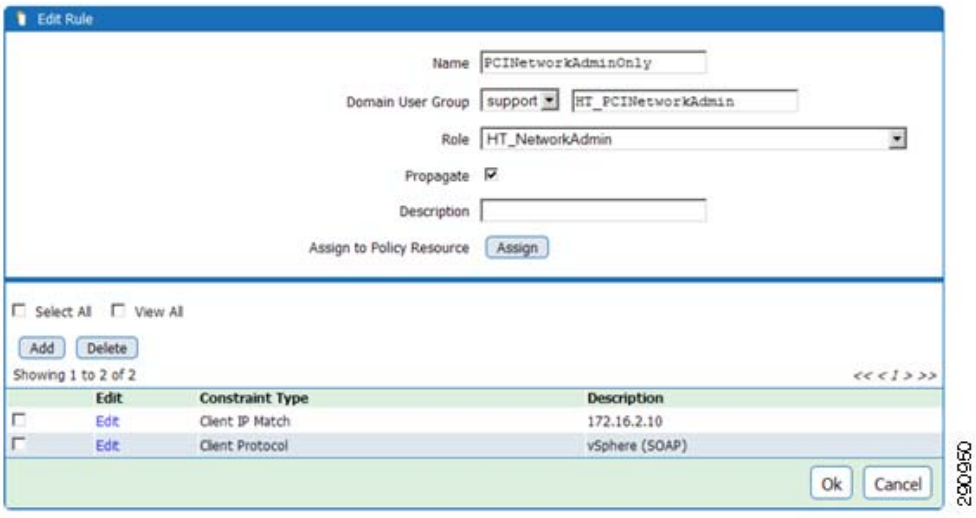
Sample Configuration

The Hytrust Appliance is designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. By integrating HyTrust Appliance authentication with Microsoft Active Directory, user accounts and passwords are not managed on the HyTrust Appliance; instead, when authentication is requested by the user, the HyTrust Appliance performs the actual authentication request against Active Directory. Complex AD environments with multiple domains are supported for authentication. Individual user IDs and roles are based on group membership.

The HyTrust Appliance implements a sophisticated policy-driven access control system that makes an authorization decision for every attempted operation in the Vblock environment. The authorization decision is based on the user ID as obtained from the vSphere session, the user function as derived from the user's assigned role in Active Directory, logical infrastructure segmentation, least privilege role defined for this activity, and object-level policy active for that user.

In the reference implementation, a policy was created that restricted virtual systems to operating only on the PHI portion of the infrastructure and enforced separation of duties between the network administrators and application owners. (See Figure 5-93.)

Figure 5-93 Edit Rule Screen



Policy and privilege definition was performed by a separate group of authorized users, typically security professionals.

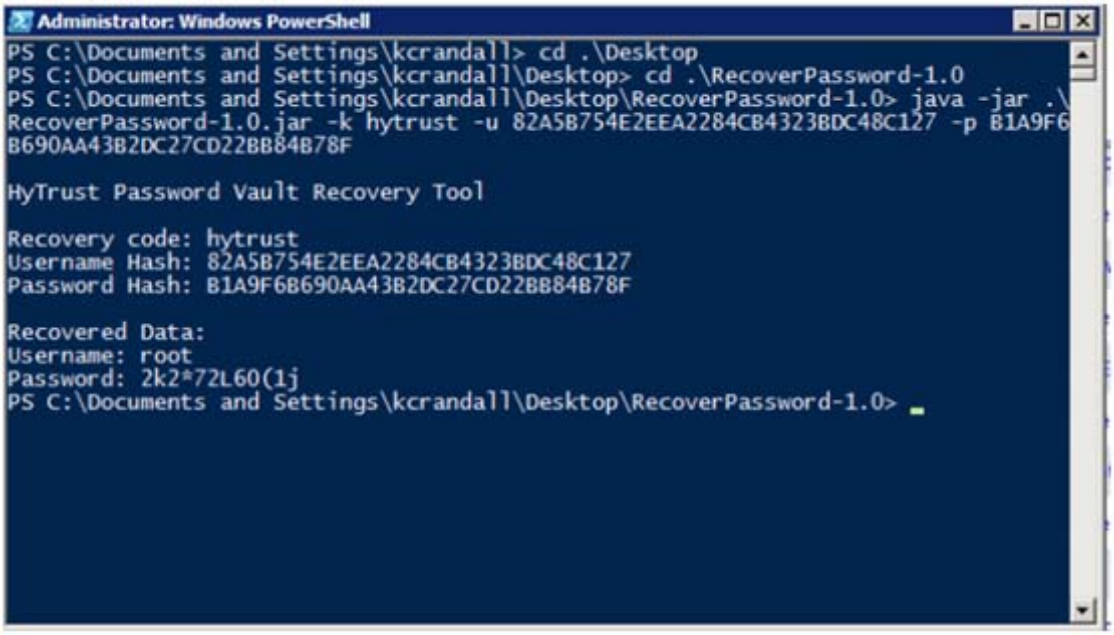
The HyTrust Appliance implements default "deny all" access policy. Many of the users that gain access to Vblock infrastructure by the means of HyTrust Appliance proxying their operations do not have privileges to log into the HyTrust Appliance management console.

RSA two-factor authentication is supported, where the user enters the AD password (something they know) in conjunction with an RSA physical token (something they have).

The HyTrust Appliance enables RSA two-factor authentication to work with any methods of access to VMware vSphere or Cisco Nexus 1000V Vblock infrastructure.

The HyTrust Appliance enforces the use of one-time root passwords for all VMware ESX hosts in the environment. Unique random machine-generated passwords of 12 characters in length are set up for each host and rotated every five days (see Figure 5-94). If requested by a privileged user, a different one-time use password was generated and remained valid for a fixed time duration not to exceed 24 hours.

Figure 5-94 Using Root Passwords

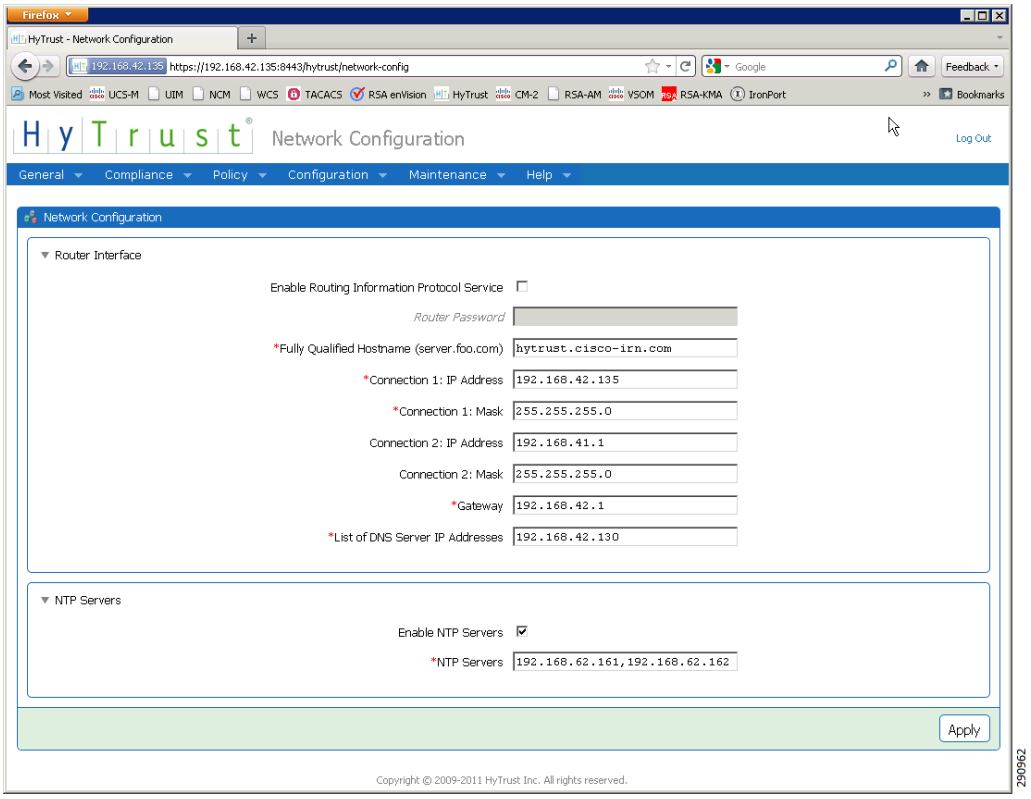


To secure authentication information and management of the HyTrust and VMware vSphere hosts, addressing Safeguard 164.308(a)(1)(i) Security Management, the HyTrust Appliance configures the virtualization platform (VMware ESX server) to disable unsecure protocols. In addition, the HyTrust Appliance proxies non-console management access and redirects attempts to connect via the HTTP management protocol to HTTPS-based connections. In the reference implementation, the configuration of VMware ESX 4.0 servers was performed in accordance with the HyTrust default configuration template. Specifically, the following controls are set:

```
ssh_config: Protocol = 2
sshd_config:
Protocol = 2
X11Forwarding = yes
IgnoreRhosts = yes
RhostsAuthentication = no
RhostsRSAAuthentication = no
HostbasedAuthentication =no
PermitRootLogin = no
PermitEmptyPasswords = no
Banner = /etc/issue.net if not set
```

As a best practice, NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. The HyTrust Appliance uses NTP by specifying the NTP server in the IP settings. (See Figure 5-95.)

Figure 5-95 Specifying the NTP Server



Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Infrastructure

Routing

Router—Clinic

The primary HIPAA function of the Cisco Integrated Services Router (ISR) is the segmentation of ePHI scope and enforcement of that new scope boundary. The ISR is the component that is used as the main routing and security platform of the clinic. It can securely scale to the requirements of the business because it has integrated firewall, VPN, and IPS/IDS capabilities. WAN options include traditional terrestrial paths using T1, T3, Ethernet, and so on; wireless options include 3G/4G/Wi-Fi modules connecting clinics over public paths for higher availability.

The Cisco ISR consolidates voice, data, and security into a single platform with local and centralized management services. It delivers scalable rich media, service virtualization, and energy efficiency ideal for deployments requiring business continuity, WAN flexibility, and superior collaboration capabilities. The Cisco ISR uses field-upgradeable motherboards, with services such as security, mobility, WAN optimization, unified communications, video, and customized applications.

Table 5-20 PHI HIPAA Assessment Summary—Cisco ISR

Models Assessed	
CISCO891W version c890-universalk9-mz.151-3.T.bin	
CISCO1941W-A/K9 version c1900-universalk9-mz.SPA.151-3.T.bin	
CISCO2921/K9 version c2900-universalk9-mz.SPA.151-3.T.bin	
CISCO2951/K9 version c2951-universalk9-mz.SPA.151-3.T.bin	
CISCO3945-SPE150/K9 version c3900-universalk9-mz.SPA.151-3.T.bin	
HIPAA Safeguards Addressed	
Administrative	**Standards/Implementation Specifications**
164.308	(a)(1)(i) Security Management Process
	(a)(3)(i) Authorization/Supervision
	(a)(4)(i) Access Authorization
	(a)(5)(i) Log-in Monitoring
	(a)(6)(i) Response and Reporting
Technical	**Standards/Implementation Specifications**
164.312	(a)(1) Access Control
	(b) Audit Controls
	(e)(2)(ii) Encryption
HIPAA Standards Failed	
No HIPAA standards were failed.	
HIPAA Implementation Specifications Failed	
No HIPAA implementation specifications were failed.	

Primary PHI Function

The primary function of the Cisco ISR is the segmentation of HIPAA scope and enforcement of that new scope boundary.

It has five primary functions/capabilities in relation to HIPAA.

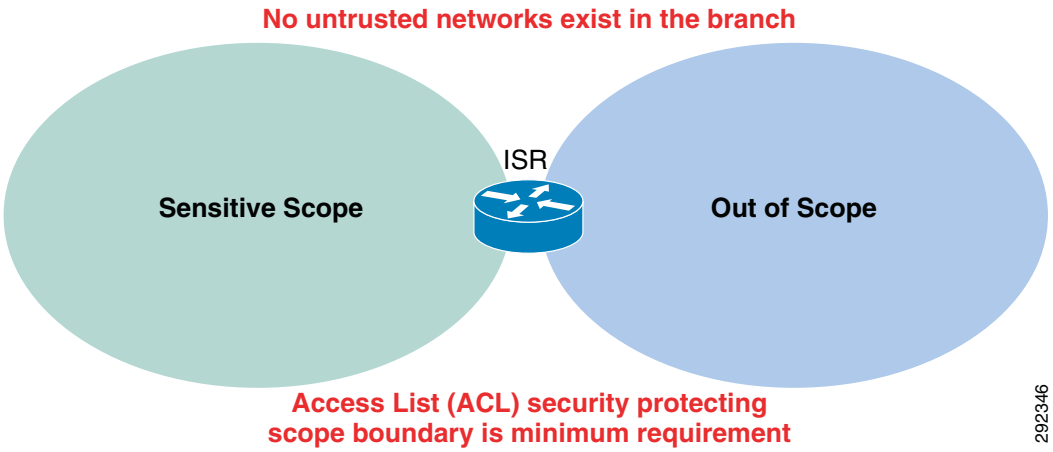
1. As a router, directing traffic between networks

   A router in its simplest form routes between networks. By segmenting a network into sub-networks, an organization can isolate sensitive information from non-sensitive information. The Cisco ISR can segment and route sensitive traffic separately from non-sensitive traffic to reduce the overall scope of a company's ePHI data environment. Depending on risk vectors within the clinic, different levels of enforcement might be required at the segmented scope boundary level. (See items 2, 3 and 4 following.)

2. As a router with ACLs, restricting traffic between the ePHI data environment and other areas of the network

   A router with ACLs can be used to enforce segmented traffic only if the ACLs are used to filter and segment private networks of the organization. They may not be used to filter untrusted networks. For example, many organizations have a central chokepoint in their data center that is the connection to the Internet (an untrusted network). As long as the organization has only untrusted network connections outside of the clinic, (the data center, in this case), then an organization may use router access lists to protect its scope from its own private internal networks. As soon as the clinic connects to untrusted networks directly, items 3 and 4 below become relevant. (See Figure 5-96.)

Figure 5-96 ACLs Segment Traffic



3. As a stateful firewall, restricting traffic between the ePHI data environment and other areas of the network

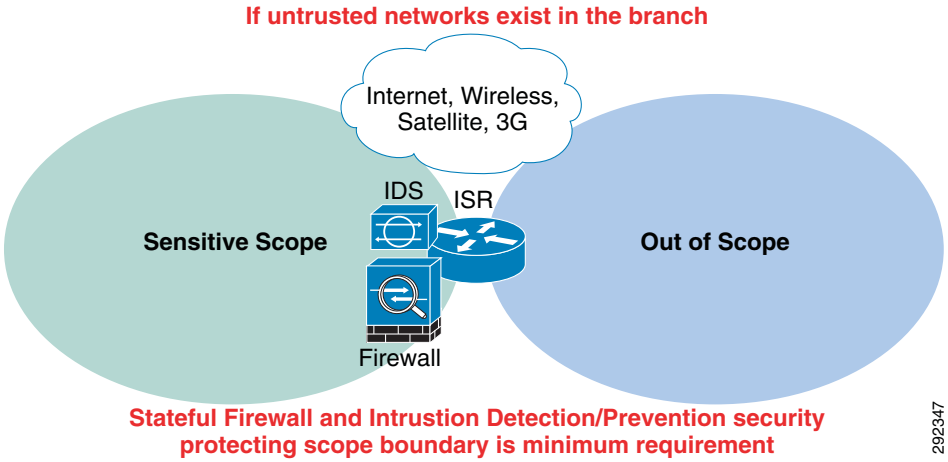
   As soon as any untrusted network is introduced at the clinic level, stateful firewalling needs to be implemented. The following are examples of untrusted networks:

   - The Internet
   - Wireless
   - Satellite
   - 3G/4G cellular backup

Step 8 As an intrusion prevention system, inspecting all traffic going to and from the ePHI data environment.

HIPAA Safeguard 164.308(a)(1)(i) requires policies and procedures to detect security violations. IDS is used to address wherever ePHI is present in the organization to detect for anomalous behavior of the sensitive area. (See Figure 5-97.)

Figure 5-97 Using Firewall and IDS/IPS



The Cisco ISR can be used to address segmentation challenges and enforce scope boundaries depending on the levels required by the organization. Each of these features can be enabled by using a license key. This feature is particularly useful for organizations because it does not require a visit to every clinic to enable the firewall/IPS/IDS capability. If these capabilities are not used within the Cisco ISR, an external component(s) can be used to address this level of scope enforcement.

4. As a VPN system, encrypting all traffic going to and from the clinic across open and public networks.

   The Cisco ISR can be used to address the need to encrypt the transmission of ePHI data across open, public networks such as 3G/4G/Wi-fi, and satellite technologies using SSL and IPSec technologies.

Design Considerations

- The security features of the Cisco ISR routers in the clinic designs are configured using Cisco Security Manager. When adopting this as the primary method of router configuration, Cisco does not recommend making changes directly to the command-line interface (CLI) of the router. Unpredictable results can occur when central and local management are used concurrently.
- The general configuration of the Cisco ISR routers in the clinic designs are maintained with Cisco Prime LMS.
- Firewall rule sets must adhere to a “least amount of access necessary” policy. Rules must be defined by specific source/destination addressing and TCP/UDP ports required for the ePHI data environment (for example, hospitals) networks.
- Enable inspection rules and/or zones on the Cisco ISR router so that the firewall maintains state (none are enabled by default).
- Redundant Cisco IOS firewalls do not have the capability to maintain state between the routers. During a failure, client communication sessions need to be re-established through the alternate router. If high availability with statefulness is a requirement, Cisco ASA firewalls should be used.

- Access into a clinic router from the WAN needs to be protected by a clinic-located firewall filter if the WAN technology is considered untrusted/public (for example, Internet DSL or cable network, public 3G or 4G, satellite). In the Cisco Solution lab, a private MPLS WAN is simulated, and filtering of the clinic traffic occurs on the WAN link of all in-scope locations.
- Disable the HTTP server service on the router and enable the HTTP secure server.
- Disable use of Telnet and enable use of only SSH version 2.
- Configure the **session-timeout** and **exec-timeout** commands to 15 minutes or less on the console, VTY, and line interfaces on the router. Disable the AUX interface.
- Configure appropriate banner messages on login, incoming, and exec modes of the router. The login banner warning should not reveal the identity of the company that owns or manages the router. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Configure the primary login authentication of the router to be directed to the Cisco Secure ACS. Individual user account profiles need to be created. Configure secondary or tertiary authentication local to the router itself in the event of a WAN or Cisco Secure ACS failure.
- Use the **no service password-recovery** command in conjunction with the **service password encryption** command to prevent password theft by physical compromise of the router.
- Change default passwords and community strings to appropriate complexity.
- Configure logs to be sent to a centralized syslog server, such as RSA enVision.
- Configure NTP to coordinate all logging.
- Disable un-necessary services (for example, Bootp, Pad, ipv6).
- Shutdown unused interfaces.

Each of the clinic designs was implemented using guidance from the following:

- Cisco Enterprise Branch Security Design Guide—
http://www.cisco.com/en/US/docs/solutions/Enterprise/Branch/E_B_SDC1.html
- Branch/WAN Design Zone—
http://www.cisco.com/en/US/netsol/ns816/networking_solutions_design_guidances_list.html

Additional information for router hardening can be found at the following URLs:

- Cisco Guide to Harden Cisco IOS Devices—
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml
- Cisco IOS Security Configuration Guide, Release 12.4—
http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4/sec_12_4_book.html
- Cisco Enterprise Branch Security Design Guide—
http://www.cisco.com/en/US/docs/solutions/Enterprise/clinic/E_B_SDC1.html
- Branch/WAN Design Zone—
http://www.cisco.com/en/US/netsol/ns816/networking_solutions_design_guidances_list.html
- Additional information for router hardening can be found at the following URLs:
- Cisco Guide to Harden Cisco IOS Devices—
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml
- Cisco IOS Security Configuration Guide, Release 12.4—
http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4/sec_12_4_book.html

HIPAA Assessment Detail—HIPAA Safeguards Addressed

All of the sample configurations of the ISR shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
  - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing
  - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
  - §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).
  - §164.312(e)(2)(ii) Encryption. Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.
- Incident response—Implement security incident response as required by HIPAA Administrative Safeguards.
  - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
  - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. Requirements addressed include: Auditing.

Sample Configuration

Cisco ISR routers are designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership. The following configurations enable central Authentication, Accounting and Authorization:

```
aaa new-model
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default
```

```
 action-type start-stop
 group tacacs+
!
aaa accounting commands 15 default
 action-type start-stop
 group tacacs+
!
aaa accounting system default
 action-type start-stop
 group tacacs+
aaa session-id common
ip tacacs source-interface Loopback0
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server domain-stripping
tacacs-server key 7 <removed>
```

Local user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration.

```
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
```

These AAA authentication groups are assigned to the administrative interfaces where users connect:

```
ip http authentication aaa login-authentication CiscoACS

line con 0
 login authentication CiscoACS

line vty 0 4
 login authentication CiscoACS

line vty 5 15
 login authentication CiscoACS
```

HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of automatic logoff options. Cisco ISR routers support session timeout. It is a best practice to set the session timeout to 15 minutes, as shown below.

```
ip http timeout-policy idle 900

line con 0
 session-timeout 15 output
 exec-timeout 15 0
line vty 0 4
 session-timeout 15 output
 exec-timeout 15 0
line vty 5 15
 session-timeout 15 output
 exec-timeout 15 0
```

Note If only the session timeout command is specified, the session timeout interval is based solely on detected input from the user. If the session timeout command is specified with the output keyword, the interval is based on both input and output traffic. You can specify a session timeout on each port. The session-timeout command behaves slightly differently on virtual (vty) terminals than on physical console, auxiliary (aux), and terminal (tty) lines. When a timeout occurs on a vty, the user session returns to the EXEC prompt. When a timeout occurs on physical lines, the user session is logged out and the line returned to the idle state. You can use a combination of the exec-timeout and session-timeout line

configuration commands, set to approximately the same values, to get the same behavior from virtual lines that the session-timeout command causes on physical lines.

To secure authentication information and management of the ISR router, addressing Safeguard 164.308(a)(1)(i) Security Management, the ISR management interfaces were configured to support HTTPS access, and SSH. Before crypto keys can be generated, hostname and domain name must be entered:

```
hostname R-A2-Small-1
ip domain name cisco-irn.com
```

Generate keys with 1024 or larger bit key generation, *not* the default 512:

```
Crypto key generate rsa 1024
```

Configure the SSH server to use the more secure protocol version SSHv2:

```
ip ssh version 2
```

Configure the HTTP server to use HTTPS, and only more secure ciphers:

```
no ip http server
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
```

Cisco ISR routers use firewalling and intrusion detection capabilities to address Safeguard 164.308(a)(1)(i) Security Management by segmenting ePHI networks from other networks and monitoring activity across these networks.

To segment ePHI information, Cisco zone-based firewalls are configured with source and destination zones to control traffic passing from one zone to another. Each of these zone pairs receives a service policy, which is the mechanism that identifies permitted traffic, while all other traffic is dropped and logged.

```
zone-pair security CSM_S_POS-W-S_POS_1 source S_POS-W destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
```

Cisco zone-based firewalls are configurable to perform stateful inspection by use of the inspect statement in the associated class map, policy map, and zone pair service policy statements.

```
class-map type inspect match-all CSM_ZBF_CLASS_MAP_9
 match access-group name CSM_ZBF_CMAP_ACL_9
 match protocol tcp

policy-map type inspect CSM_ZBF_POLICY_MAP_7
 class type inspect CSM_ZBF_CLASS_MAP_9
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_10
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_11
  inspect Inspect-1
 class class-default
  drop log
```

In the clinic, VLANs are used to segment traffic based on function and security requirements. Each of these VLANs are assigned to an appropriate security zone using the zone-based firewall feature of the router.

```
interface GigabitEthernet0/0.11
  description POS
  zone-member security S_POS
interface GigabitEthernet0/0.13
  description VOICE
```

```
 zone-member security S_Voice
```

Cisco routers are capable of performing intrusion detection. Each of the reference designs includes networks where intrusion detection capabilities are required. IPS signature updates and configurations are managed centrally through Cisco Security Manager, which implements the following configuration statements to enable the IPS inspection capability in the routers:

```
ip ips config location flash0: retries 1 timeout 1
ip ips notify SDEE
ip ips name CISCO-IPS
!
ip ips signature-category
 category all
  retired true
 category ios_ips default
  retired false
!
interface GigabitEthernet0/0
 description WAN
 ip ips CISCO-IPS in
 ip ips Store-IPS out
interface GigabitEthernet0/1.11
 description POS
 ip ips CISCO-IPS in
 ip ips CISCO-IPS out
interface GigabitEthernet0/1.15
 description WIRELESS-POS
 ip ips CISCO-IPS in
 ip ips CISCO-IPS out
```

To address the Incident Response and Auditing HIPAA safeguards identified above, Cisco ISR routers can be configured to send log data to the RSA enVision log management platform. Cisco routers track individual administrator actions through several mechanisms including AAA, logging, and system events by implementing the following configuration statements:

```
logging trap debugging
logging 192.168.42.124
logging buffered 50000

login on-failure log
login on-success log

archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
```

And SNMP:

```
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps flash insertion removal
snmp-server enable traps energywise
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
snmp-server enable traps hsrp
```

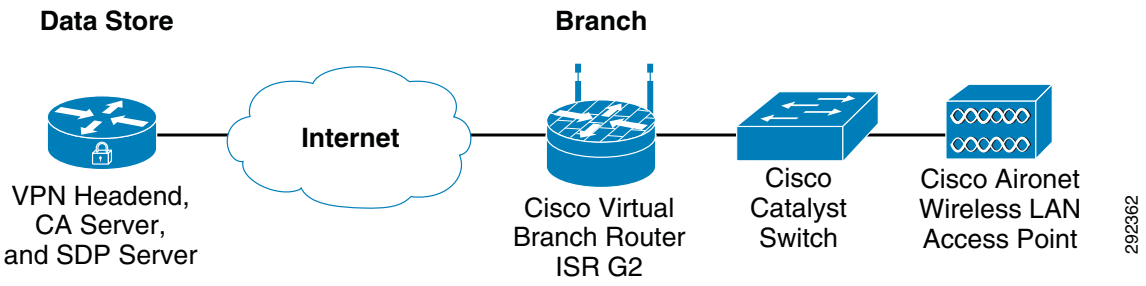
```
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps ipsla
snmp-server host 192.168.42.124 remoteuser
```

Public WAN link connections include technologies such as DSL, cable, satellite, Wi-Fi, and 3G/4G networks. These are public networks and Safeguard §164.312(e)(2)(ii) Encryption specifies that electronic protected health information is to be encrypted. A VPN is required to securely tunnel traffic between the clinic and the enterprise network across these mediums.

Cisco Virtual Office provides reference designs for building a VPN solution to connect clinics to data centers using these technologies. For more information about Cisco VPN solutions, see: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6660/ps6808/prod_white_paper0900aecd8051bf3b_ns855_Networking_Solutions_White_Paper.html.

The following example describes equipment located at the clinic and the data center headend router. The clinic router is referred to as the spoke router, and the data center router as the hub. Figure 5-98 shows a simplified Cisco VPN topology.

Figure 5-98 Cisco VPN Topology



Cisco VPN technology connects the clinics to the data center over the Internet. As a result, a secure, encrypted tunnel is used to secure sensitive information such as ePHI data. Cisco VPN technologies offer a choice to protect the data in transit and provide a secure access to the clinics' networks, including Easy VPN and Dynamic Multipoint VPN (DMVPN).

This example shows DMVPN as the VPN technology. DMVPN uses IPSec-encrypted GRE tunnels, with dynamic routing. Two simultaneously active DMVPN tunnels are built from each clinic to different hub routers, providing instant failover. If the primary tunnel fails, routing converges to use the secondary tunnel, and all sessions are kept alive. In addition, with DMVPN, clinic routers can dynamically build spoke-to-spoke tunnels between each other to exchange data, without having to tunnel the traffic back to the hub, thus alleviating the load on the headend.

Following are sample DMVPN spoke and hub configurations. Enhanced Interior Gateway Routing Protocol (EIGRP) is used as the routing protocol inside the DMVPN network. Split-tunneling is used and only traffic on the POS and employee VLANs going to the servers on the 10.0.0.0 network at the headquarters is sent through the DMVPN tunnel, while any other traffic is sent straight to the Internet. Note that, if split-tunneling is not required, a default route (to 0.0.0.0) can be advertised from the hubs to the spokes, instead of specific subnets.

891 Clinic Router

```
!! Configure the IP addresses on the VLAN interfaces
interface vlan 10
  description POS VLAN
  ip address 172.16.10.1 255.255.255.0
```

```
  no autostate
interface vlan 20
  description employee VLAN
  ip address 172.16.20.1 255.255.255.0
  no autostate
interface vlan 30
  description guest VLAN
  ip address 172.16.30.1 255.255.255.0
  no autostate
!! Configure the ISAKMP and IPSec policies
crypto isakmp policy 1
  encryption aes 256

crypto isakmp keepalive 35 5
crypto isakmp nat keepalive 10
crypto ipsec transform-set t1 esp-aes 256 esp-sha-hmac
 mode transport

crypto ipsec profile cvs
 set transform-set t1
ip multicast-routing
!! Configure the DMVPN tunnel
interface Tunnel0
  bandwidth 1000
  ip address 192.168.1.3 255.255.255.0
  no ip redirects
  ip mtu 1400
  ip hello-interval eigrp 99 30
  ip hold-time eigrp 99 90
  ip pim sparse-dense-mode
  ip nhrp map multicast <Primary-hub-public-IP>
  ip nhrp map 192.168.1.1 <Primary-hub-public-IP>
  ip nhrp nhs 192.168.1.1
  ip nhrp map multicast <Secondary-hub-public-IP>
  ip nhrp map 192.168.1.2 <Secondary-hub-public-IP>
  ip nhrp nhs 192.168.1.2
  ip nhrp authentication <password>
  ip nhrp network-id 12345
  ip nhrp holdtime 300
  ip nhrp registration no-unique
  ip nhrp shortcut
  ip nhrp redirect
  ip tcp adjust-mss 1360
  load-interval 30
  delay 1000
  qos pre-classify
  tunnel source GigabitEthernet0
  tunnel mode gre multipoint
  tunnel key 12345
  tunnel protection ipsec profile cvs


!! Configure the DMVPN routing protocol. Only permit the POS and employee LAN !!
subnets to be advertised to the hubs
ip access-list standard dmvpn_acl
  permit 172.16.10.0 0.0.0.255
  permit 172.16.20.0 0.0.0.255

router eigrp 99
  no auto-summary
  network 192.168.1.3 0.0.0.0
  network 172.16.10.1 0.0.0.0
  network 172.16.20.1 0.0.0.0
  distribute-list dmvpn_acl out
```

3945E Hub Router

```
!! Configure the ISAKMP and IPSec policies

crypto isakmp policy 1
  encryption aes 256

crypto isakmp keepalive 35 5
crypto isakmp nat keepalive 10

crypto ipsec transform-set t1 esp-aes 256 esp-sha-hmac
  mode transport require

crypto ipsec profile cvs
  set transform-set t1

!! Enable multicast routing

ip multicast-routing

!! Configure the DMVPN tunnel. Use the same bandwidth metric for both primary !! and
secondary hubs, but a lower delay metric on the primary hub

interface Tunnel0

  bandwidth 2000
  ip address 192.168.1.1 255.255.255.0
  no ip redirects
  ip mtu 1400
  ip pim sparse-dense-mode
  ip nhrp authentication <password>
  ip nhrp map multicast dynamic
  ip nhrp network-id 12345
  ip nhrp redirect
  ip tcp adjust-mss 1360
  no ip split-horizon eigrp 99
  delay 1000
  qos pre-classify
  tunnel source <Outside_Interface >
  tunnel mode gre multipoint
  tunnel key 12345
  tunnel protection ipsec profile cvs

!! Configure the DMVPN routing protocol. Only the 10.0.0.0 network is        !!
advertised to the spokes in this example (split-tunneling)

router eigrp 99
  no auto-summary
  network 192.168.1.1 0.0.0.0
  redistribute static route-map split_in
ip access-list standard split_in
  permit 10.0.0.0

route-map split_in permit 10
  match ip address split_in
```

As a best practice, NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the

data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. Cisco routers use NTP to meet these requirements by implementing the following configuration statements:

```
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162

clock timezone PST -8 0
clock summer-time PDT recurring

service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
```

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Routers—Data Center

The primary function of data center routers from a HIPAA perspective is routing between ePHI networks and out-of scope networks and enforcing that boundary with firewall services. Data center routers function as WAN aggregation routers or connecting to larger networks such as the Internet. Therefore, performance and scalability are equally important as securely passing data. For this reason, and unlike the routers in the clinic, security functions are typically separated physically into distinct appliances. The Cisco ASR routers were used for the Internet edge and clinic WAN edge portions of the network within the solution testing.

Table 5-21 PHI HIPAA Assessment Summary—Cisco ASR

Models Assessed	
ASR-1002 (RP1) version asr1000rp1-adventerprisek9.03.02.01.S.151-1.S1.bin	
HIPAA Safeguards Addressed	
Administrative	**Standards/Implementation Specifications**
164.308	(a)(1)(i) Security Management Process
	(a)(3)(i) Authorization/Supervision
	(a)(4)(i) Access Authorization
	(a)(5)(i) Log-in Monitoring
	(a)(6)(i) Response and Reporting
Technical	**Standards/Implementation Specifications**
164.312	(a)(i) Access Control
	(b) Audit Controls
HIPAA Standards Failed	

Table 5-21 PHI HIPAA Assessment Summary—Cisco ASR (continued)

No HIPAA standards were failed.
HIPAA Implementation Specifications Failed
No HIPAA implementation specifications were failed.

Primary ePHI Function

The primary function of the data center routers is the segmentation of ePHI scope and enforcement of that new scope boundary. The data center router has four primary functions/capabilities in relation to HIPAA:

1. As a router, directing traffic between networks

   A router in its simplest form routes between networks. By segmenting a network into sub-networks, an organization can isolate sensitive information from non-sensitive information. Data center routers can segment and route sensitive traffic separately from non-sensitive traffic to reduce the overall scope of a company's HIPAA ePHI environment. Depending on risk vectors, different levels of enforcement might be required at the segmented scope boundary level. (See items 2, 3, and 4 following.)

2. As a router with ACLs, restricting traffic between the ePHI networks and other areas of the network

   A router with ACLs can be used to enforce segmented traffic only if the ACLs are used to filter and segment private networks of the organization. They may not be used to filter untrusted networks. For example, if a data center router is used to segment sensitive ePHI networks from other internal networks, an organization may use router access lists to protect its scope. As soon as this segment connects to untrusted networks directly, item number 3 becomes relevant.

3. As a stateful firewall, restricting traffic between the ePHI environment and other untrusted areas.

   As soon as any untrusted network is introduced to the connections of the data center router, firewalling must be deployed. The following are examples of untrusted networks:

   - Internet
   - Wireless
   - Satellite
   - Cellular backup

4. As an intrusion prevention system, inspecting all traffic going to and from the ePHI environment. HIPAA Safeguard 164.308(a)(1)(i) requires policies and procedures to detect security violations. IDS is used to address wherever ePHI is present in the organization to detect for anomalous behavior of the sensitive area.

Design Considerations

- Configuration was done manually on the router CLI, and backup of configuration and monitoring of configuration for changes and non-compliance were done through Cisco Prime LMS (alternatively, CiscoWorks Resource Manager Essentials, a component of Cisco LMS, can be used as well).
- Disable the HTTP server service on the router and enable the HTTP secure server.
- Configure the **session-timeout** and **exec-timeout** commands to 15 minutes or less on the console, VTY, and line interfaces on the router. Disable the AUX interface.

- Configure appropriate banner messages on login, incoming, and exec modes of the router. The login banner warning should not reveal the identity of the company that owns or manages the router. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Configure the primary login authentication of the router to be directed to the Cisco Secure ACS. Individual user account profiles need to be created. Configure secondary or tertiary authentication local to the router itself in the event of a WAN or Cisco Secure ACS failure.
- Use the **no service password-recovery** command in conjunction with the **service password encryption** command to prevent password theft by physical compromise of the router.
- Enable anti-spoofing on all interfaces.
- Routers in the data center were implemented using guidance from the following:
  - Enterprise Data Center Design guide based on a Data Center 3.0 Architecture—http://www.cisco.com/en/US/netsol/ns743/networking_solutions_program_home.html
  - Enterprise Internet Edge Design Guide—http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/IE_DG.html
- For the Internet edge routers, use the access list below on the interface that is facing the Internet. This access list explicitly filters traffic destined for the infrastructure address space. Deployment of edge infrastructure access lists requires that you clearly define your infrastructure space and the required/authorized protocols that access this space. The access list is applied at the ingress to your network on all externally facing connections, such as peering connections, customer connections, and so forth.

```
!
ip access-list extended COARSE-FILTER-INTERNET-IN
 remark ------------------------------------
 remark ---Block Private Networks---
 deny   ip 10.0.0.0 0.255.255.255 any log
 deny   ip 172.16.0.0 0.15.255.255 any log
 deny   ip 192.168.0.0 0.0.255.255 any log
 remark -
 remark ---Block Autoconfiguration Networks---
 deny   ip 169.254.0.0 0.0.255.255 any log
 remark -
 remark ---Block Loopback Networks---
 deny   ip 127.0.0.0 0.0.255.255 any log
 remark -
 remark ---Block Multicast Networks---
 deny   ip 224.0.0.0 15.255.255.255 any log
 remark -
 remark ---Block Your assigned IP's at edge---
 deny   ip <YOUR_CIDR_BLOCK> any log
 remark -
 remark ---Allow remaining public internet traffic---
 permit ip any any
!
```

Note The **log** keyword can be used to provide additional details about source and destinations for a given protocol. Although this keyword provides valuable insight into the details of access list hits, excessive hits to an access list entry that uses the **log** keyword increase CPU utilization. The performance impact associated with logging varies by platform.

HIPAA Assessment Detail—HIPAA Safeguards Addressed

All of the sample configurations of the Cisco ASR shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
  - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing
  - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
  - §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
  - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
  - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. Requirements addressed include: Auditing.

Sample Configuration

Cisco ASR routers are designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership. The following configurations enable central Authentication, Accounting and Authorization:

```
aaa new-model
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
aaa session-id common
```

```
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
```

Local user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration.

```
username bart privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 4 <removed>
username csmadmin privilege 15 secret 4 <removed>
```

These AAA authentication groups are assigned to the administrative interfaces where users connect:

```
ip http authentication aaa login-authentication CiscoACS

line con 0
 login authentication CiscoACS

line vty 0 4
 login authentication CiscoACS

line vty 5 15
 login authentication CiscoACS
```

HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of automatic logoff options. Cisco ASR Routers support session timeout. It is a best practice to set the session timeout to 15 minutes, as shown below.

```
ip http timeout-policy idle 60 life 86400 requests 10000
line con 0
session-timeout 15 output
exec-timeout 15 0
line vty 0 4
session-timeout 15 output
exec-timeout 15 0
line vty 5 15
session-timeout 15 output
exec-timeout 15 0
```

Note If only the session timeout command is specified, the session timeout interval is based solely on detected input from the user. If the session timeout command is specified with the output keyword, the interval is based on both input and output traffic. You can specify a session timeout on each port. The session-timeout command behaves slightly differently on virtual (vty) terminals than on physical console, auxiliary (aux), and terminal (tty) lines. When a timeout occurs on a vty, the user session returns to the EXEC prompt. When a timeout occurs on physical lines, the user session is logged out and the line returned to the idle state. You can use a combination of the exec-timeout and session-timeout line configuration commands, set to approximately the same values, to get the same behavior from virtual lines that the session-timeout command causes on physical lines.

To secure authentication information and management of the ASR router, addressing Safeguard 164.308(a)(1)(i) Security Management, the ASR management interfaces were configured to support HTTPS access, and SSH. Before crypto keys can be generated hostname and domain name must be entered:

```
hostname RWAN-1
ip domain name cisco-irn.com
```

Generate keys with 1024 or larger bit key generation, *not* the default 512.

```
Crypto key generate rsa 1024
```

Configure the SSH server to use the more secure protocol version SSHv2.

```
ip ssh version 2
```

Configure the HTTP server to use HTTPS, and only more secure ciphers:

```
no ip http server
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
```

Configure the use of Secure Copy in place of TFTP:

```
ip scp server enable
```

To address the Incident Response and Auditing HIPAA safeguards identified above, Cisco ASR Routers can be configured to send log data to the RSA enVision log management platform. Cisco routers track individual administrator actions through several mechanisms including AAA, logging, and system events by implementing the following configuration statements:

```
logging trap debugging
logging 192.168.42.124
logging buffered 50000

login on-failure log
login on-success log

archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
```

And SNMP:

```
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0snmp-server enable traps snmp authentication linkdown
linkup coldstart warmstart
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps flash insertion removal
snmp-server enable traps energywise
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps ipsla
snmp-server host 192.168.42.124 remoteuser
```

As a best practice, NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the

data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. Cisco routers use NTP to meet these requirements by implementing the following configuration statements:

```
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162

clock timezone PST -8 0
clock summer-time PSTDST recurring

service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
```

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Switching

Switches—Clinic

Cisco branch switches provide connectivity for wired endpoints and the ability to segment them onto their own sensitive scope networks. Virtual local area networks (VLANs) are used to put sensitive ePHI applications and devices onto their own network and segregate them from devices that are on non-sensitive networks.

- Cisco branch switches are stackable, expandable switches that can be used for wired device port density in branch wiring closets. Access switches offer a variety of modular and fixed configuration options, and feature operational efficiency with StackPower, FlexStack, and NetFlow to increase visibility and control
- Core/distribution—Highly redundant, powerful core switches allow for the most demanding business requirements of the healthcare organization. Modular functionality provides the ability to insert security technology as the needs of the business expand into new areas.

Table 5-22 PHI HIPAA Assessment Summary—Cisco Clinic Switches

Models Assessed	
WS-C3560E-PS-24 c3560e-universalk9-mz.122-35.SE5.bin WS-C2960PD-8TT-L c2960-lanbasek9-mz.122-55.SE1.bin WS-C2960G-8TC-L c2960-lanbasek9-mz.122-50.SE4.bin WS-C2960-8TC-L c2960-lanbasek9-mz.122-50.SE4.bin WS-C2960S-48FPS-L c2960s-universalk9-mz.122-53.SE1.bin WS-C3750X-48PF-S c3750e-universalk9-mz.122-53.SE2.bin WS-C2960CPD-8PT-L c2960c405-universalk9-mz.122-55.0.43.SK.bin WS-4507+R SUP-7 cat4500e-universalk9.SPA.03.01.00.SG.150-1.XO.bin WS-C3560X-48PF-S c3560e-universalk9-mz.122-53.SE2.bin WS-C3560CPD-8PT-L c3560c405ex-universalk9-mz.122-55.0.44.SK.bin	
HIPAA Safeguards Addressed	
Administrative	**Standards/Implementation Specifications**
164.308	(a)(1)(i) Security Management Process
	(a)(3)(i) Authorization/Supervision
	(a)(4)(i) Access Authorization
	(a)(5)(i) Log-in Monitoring
	(a)(6)(i) Security Incident Procedures
	(a)(6)(ii) Response and Reporting
Technical	**Standards/Implementation Specifications**
164.312	(a)(1) Access Control
	(b) Audit Controls
	(c)(1) Data Integrity
	(e)(i) Transmission Security
	(e)(2)(i) Integrity Controls.
	(e)(2)(ii) Encryption
HIPAA Standards Failed	
No HIPAA standards were failed.	
HIPAA Implementation Specifications Failed	
No HIPAA implementation specifications were failed.	

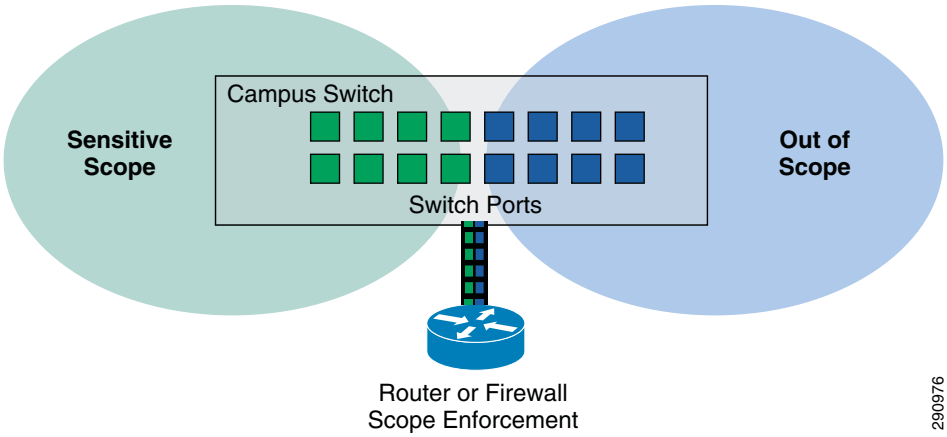
Primary PHI Function

The primary HIPAA compliance feature of clinic switches is to provide secure wired port access.

Clinic switches also provide compliance via segmentation of sensitive networks from out-of-scope networks. Switches extend that Layer 3 boundary to Layer 2. Using VLANs, Cisco clinic switches allow organizations to put their networks into separate VLANs (scopes) from other non-sensitive data (out-of-scope).

Figure 5-99 shows an example of switch segmentation.

Figure 5-99 Cisco Branch Switch Segmentation



Although the enforcement of these boundaries would be handled by either a router or firewall, the switch provides the port density and access required to connect the devices from the clinic floor.

Design Considerations

- The configurations of the Cisco Catalyst switches in the clinic architectures are maintained within Cisco Prime LMS (alternatively CiscoWorks Resource Manager Essentials, a component of C-LMS, can be used as well).
- The use of VLANs on the Cisco Catalyst switch enables the organization to provide same-box wired access to its devices while maintaining segregated addressing schemes.
- Disable the HTTP server on the switch and enable the HTTP secure server.
- Using the stacking capability of Cisco Catalyst switches improves high availability designs while simplifying configuration and support.
- Cisco SmartPorts simplifies connecting the right device to the right VLAN.
- Network Admission Control (NAC) protects the network from rogue devices being connected.
- Cisco compact switches can easily add more securely managed ports where needed (for example, Cash Wrap and customer service desk), and some models can use PoE.
- Set the **session** and **exec timeout** commands to 15 minutes or less.
- Configure appropriate banner messages on login, incoming, and exec modes of the switch. The login banner warning should not reveal the identity of the company that owns or manages the switch. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Configure the primary login authentication of the switch to be directed to the Cisco Secure ACS. Individual user account profiles need to be created. Configure secondary or tertiary authentication local to the switch itself in the event of a WAN or Cisco Secure ACS failure.
- Use the **no service password-recovery** command in conjunction with the **service password encryption** command to prevent password theft by physical compromise of the switch.

HIPAA Assessment Detail—HIPAA Safeguards Addressed

All of the sample configurations of the Cisco clinic switches shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
  - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
  - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. Requirements addressed include: Auditing.
  - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
- Integrity—Protect electronic protected health information from improper alteration or destruction as required by HIPAA Technical safeguards.
  - §164.312(c)(1) Data Integrity. Implement policies and procedures to protect health information from improper alteration or destruction.
  - §164.312(e)(1) Transmission Security. Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network. Requirements addressed include: Encryption and Integrity.
  - §164.312(e)(2)(i) Integrity Controls. Implement security measures to ensure that ePHI is not improperly modified without detection until disposed of. Requirements addressed include: Integrity.
  - §164.312(e)(2)(ii) Encryption. Implement a mechanism to encrypt ePHI whenever deemed appropriate. Requirements addressed include: Encryption.
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
  - §164.308(a)(6)(i) Security Incident Procedures. Implement policies and procedures to address security incidents.
  - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.

Sample Configuration

Cisco switches are designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership.

```
aaa new-model
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
aaa session-id common
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server domain-stripping
tacacs-server key 7 <removed>
```

Local individual user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration.

```
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
```

These AAA authentication groups are assigned to the administrative interfaces where users connect.

```
ip http authentication aaa login-authentication CiscoACS

line con 0
 login authentication CiscoACS

line vty 0 4
 login authentication CiscoACS

line vty 5 15
 login authentication CiscoACS
```

HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of automatic logoff options. Cisco Clinic switches supports session timeout. It is a best practice to set the session timeout to 15 minutes, as shown below.

```
ip http timeout-policy idle 900

line con 0
 session-timeout 15 output
 exec-timeout 15 0
line vty 0 4
 session-timeout 15 output
 exec-timeout 15 0
line vty 5 15
 session-timeout 15 output
 exec-timeout 15 0
```

To secure authentication information and management of the clinic switch, addressing Safeguard 164.308(a)(1)(i) Security Management, the clinic switch management interfaces were configured to support HTTPS access, and SSH. Before crypto keys can be generated hostname and domain name must be entered:

```
hostname S-A2-MED-1/2
ip domain name cisco-irn.com
```

Generate keys with 1024 or larger bit key generation, *not* the default 512.

```
Crypto key generate rsa 1024
```

Configure the SSH server to use the more secure protocol version SSHv2:

```
ip ssh version 2
```

Configure the HTTP server to use HTTPS, and only more secure ciphers:

```
no ip http server
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
```

Configure the use of Secure Copy in place of TFTP:

```
ip scp server enable
```

Cisco switches are able to track and monitor all administrative user access, events such as port up/down, as well as device authentication events when using 802.1x. See Cisco ISE for more information regarding port authentication.

To address the Incident Response and Auditing HIPAA safeguards identified above, Cisco Switches can be configured to send log data to the RSA enVision log management platform. Cisco switches track individual administrator actions through several mechanisms including AAA, logging, and system events by implementing the following configuration statements:

```
logging trap debugging
logging 192.168.42.124
logging buffered 50000

login on-failure log
login on-success log


archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
```

And SNMP:

```
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan
no-guest-vlan
snmp-server enable traps energywise
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps power-ethernet group 1-4
snmp-server enable traps power-ethernet police
snmp-server enable traps cpu threshold
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps envmon fan shutdown supply temperature status
```

```
snmp-server enable traps errdisable
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server host 192.168.42.124 remoteuser
```

As a best practice, NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. Cisco switches use NTP to meet these requirements by implementing the following configuration statements:

```
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162

clock timezone PST -8 0
clock summer-time PSTDST recurring

service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
```

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Cisco Catalyst Switches—Data Center

The Cisco Catalyst family of data center switches are designed to securely switch data from servers to high speed trunks, maintaining the integrity of segmented scopes of compliance. They provide scalable inter-switch connectivity, high port density for wired endpoints, and the ability to segment them into sensitive scope networks. VLANs are used to put sensitive ePHI applications and devices onto their own network and segregate them from devices that are on non-sensitive networks. Data center Cisco Catalyst switches are highly redundant, capable of delivering high performance switching, with feature options depending on the needs of the business.

Modular functionality provides the ability to insert security technology to enforce compliance needs.

- Security services include access control, firewall, and intrusion prevention.
- Wireless services can be aggregated into these switches for central policy control of unified wireless access points.
- Application services include quality of service (QoS), content filtering, and load balancing.

Table 5-23 PHI HIPAA Assessment Summary—Cisco Data Center Switches

Models Assessed
Cisco Catalyst6509-Sup720-3BXL version s72033-adventerprisek9_wan-mz.122-33.SXJ.bin WS-C3750-48P version c3750-ipbasek9-mz.122-55.SE1.bin

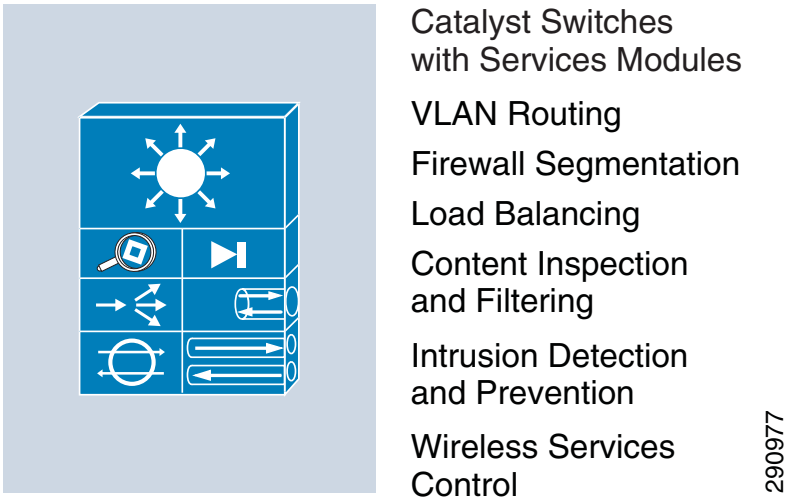
Table 5-23 PHI HIPAA Assessment Summary—Cisco Data Center Switches

HIPAA Safeguards Addressed	
Administrative	**Standards/Implementation Specifications**
164.308	(a)(1)(i) Security Management Process
	(a)(3)(i) Authorization/Supervision
	(a)(4)(i) Access Authorization
	(a)(5)(i) Log-in Monitoring
	(a)(6)(i) Security Incident Procedures
	(a)(6)(ii) Response and Reporting
Technical	**Standards/Implementation Specifications**
164.312	(a)(1) Access Control
	(b) Audit Controls
	(c)(1) Data Integrity
	(e)(i) Transmission Security
	(e)(2)(i) Integrity Controls.
	(e)(2)(ii) Encryption
HIPAA Standards Failed	
No HIPAA standards were failed.	
HIPAA Implementation Specifications Failed	
No HIPAA implementation specifications were failed.	

Primary PHI Function

Securing the infrastructure is a key PHI compliance feature of Cisco Catalyst data center switches. Cisco Catalyst switches have firewall/IDS modules for perimeter security. (See Figure 5-100.)

Figure 5-100 Cisco Catalyst Data Center Switches



The primary function of the Cisco Catalyst data center switches is segmentation of scope and enforcement of that new scope boundary. These switches have five primary functions/capabilities in relation to HIPAA:

- Using VLANs, Cisco Catalyst switches allow an organization to put its ePHI networks into separate VLANs (scopes) from other non-sensitive data (out of scope).
- The Layer 3 Cisco Catalyst switch acts as a router, directing traffic between networks. By segmenting a network into sub-networks, an organization can isolate sensitive information from non-sensitive information. The Cisco Catalyst switch can perform the ability to segment and route sensitive traffic from non-sensitive and reduce the overall scope of a company's ePHI data environment. Depending on risk vectors, different levels of enforcement are required at the segmented scope boundary level. See the following bullets for details.
- The Layer 3 Cisco Catalyst switch acts as a router with ACLs, restricting traffic between the ePHI data environment and other areas of the network. A Cisco Catalyst switch with ACLs can be used to enforce segmented traffic if the ACLs are used only to filter and segment private networks of the organization. ACLs may not be used to segment untrusted networks.
- The Cisco Catalyst switch with a firewall service module restricts traffic between the ePHI data environment and other areas of the network. As soon as any untrusted network is introduced, firewalling must be deployed.
- The Layer 3 Cisco Catalyst switch with an intrusion prevention module inspects all traffic going to and from the ePHI data environment. HIPAA Safeguard 164.308(a)(1)(i) requires policies and procedures to detect security violations. IDS is used to address wherever ePHI is present in the organization to detect for anomalous behavior of the sensitive area.

Design Considerations

- The configurations of the Cisco Catalyst switches in the data center and Internet edge architectures are maintained within Cisco Prime LMS (alternatively CiscoWorks Resource Manager Essentials, a component of C-LMS, can be used as well).
- The use of VLANs on the Cisco Catalyst switch enables the organization to provide same-box wired access to its devices while maintaining segregated addressing schemes.
- Using the stacking capability of Cisco Catalyst switches improves high availability designs while simplifying configuration and support.
- Disable the HTTP server on the switch and enable the HTTP secure server.
- Set the **session** and **exec timeout** commands to 15 minutes or less.
- Configure appropriate banner messages on login, incoming, and exec modes of the switch. The login banner warning should not reveal the identity of the company that owns or manages the switch. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Configure the primary login authentication of the switch to be directed to the Cisco Secure ACS. Individual user account profiles need to be created. Configure secondary or tertiary authentication local to the switch itself in the event of a WAN or Cisco Secure ACS failure.
- Use the **no service password-recovery** command in conjunction with the **service password encryption** command to prevent password theft by physical compromise of the switch.

HIPAA Assessment Detail—HIPAA Safeguards Addressed

All of the sample configurations of the Cisco Catalyst data center switches shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
  - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
  - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. Requirements addressed include: Auditing.
  - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
- Integrity—Protect electronic protected health information from improper alteration or destruction as required by HIPAA Technical safeguards.
  - §164.312(c)(1) Data Integrity. Implement policies and procedures to protect health information from improper alteration or destruction.
  - §164.312(e)(1) Transmission Security. Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network. Requirements addressed include: Encryption and Integrity.
  - §164.312(e)(2)(i) Integrity Controls. Implement security measures to ensure that ePHI is not improperly modified without detection until disposed of. Requirements addressed include: Integrity.
  - §164.312(e)(2)(ii) Encryption. Implement a mechanism to encrypt ePHI whenever deemed appropriate. Requirements addressed include: Encryption.
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
  - §164.308(a)(6)(i) Security Incident Procedures. Implement policies and procedures to address security incidents.
  - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.

Sample Configuration

Cisco switches are designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership.

```
aaa new-model
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
aaa session-id common
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server domain-stripping
tacacs-server key 7 <removed>
```

Local individual user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration.

```
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
```

These AAA authentication groups are assigned to the administrative interfaces where users connect.

```
ip http authentication aaa login-authentication CiscoACS

line con 0
 login authentication CiscoACS

line vty 0 4
 login authentication CiscoACS

line vty 5 15
 login authentication CiscoACS
```

HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of automatic logoff options. Cisco data center switches support session timeout. It is a best practice to set the session timeout to 15 minutes, as shown below.

```
ip http timeout-policy idle 900

line con 0
 session-timeout 15 output
 exec-timeout 15 0
line vty 0 4
 session-timeout 15 output
 exec-timeout 15 0
line vty 5 15
 session-timeout 15 output
 exec-timeout 15 0
```

To secure authentication information and management of the Cisco data center switches, addressing Safeguard 164.308(a)(1)(i) Security Management, the Cisco data center switches management interfaces were configured to support HTTPS access, and SSH. Before crypto keys can be generated hostname and domain name must be entered:

```
hostname S-A2-MED-1/2
ip domain name cisco-irn.com
```

Generate keys with 1024 or larger bit key generation, *not* the default 512.

```
Crypto key generate rsa 1024
```

Configure the SSH server to use the more secure protocol version SSHv2:

```
ip ssh version 2

Configure the HTTP server to use HTTPS, and only more secure ciphers:
no ip http server
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
```

Configure the use of Secure Copy in place of TFTP

```
ip scp server enable
```

Cisco switches are able to track and monitor all administrative user access, events such as port up/down, as well as device authentication events when using 802.1x. See Cisco ISE for more information regarding port authentication.

To address the Incident Response and Auditing HIPAA safeguards identified above, Cisco Switches can be configured to send log data to the RSA enVision log management platform. Cisco switches track individual administrator actions through several mechanisms including AAA, logging, and system events by implementing the following configuration statements:

```
logging trap debugging
logging 192.168.42.124
logging buffered 50000

login on-failure log
login on-success log


archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
```

And SNMP:

```
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan
no-guest-vlan
snmp-server enable traps energywise
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps power-ethernet group 1-4
snmp-server enable traps power-ethernet police
snmp-server enable traps cpu threshold
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps errdisable
```

```
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server host 192.168.42.124 remoteuser
```

As a best practice, NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. Cisco switches use NTP to meet these requirements by implementing the following configuration statements:

```
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162

clock timezone PST -8 0
clock summer-time PSTDST recurring

service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
```

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Cisco Nexus 1000V Switch—Data Center

The Cisco Nexus 1000V Series Switch provides connectivity for virtual servers with the ability to segment them onto their own sensitive scope networks. VLANs are used to put sensitive PHI applications and devices onto their own network and segregate them from devices that are on non-sensitive networks.

The Cisco Nexus 1000V Series Switch provides advanced networking functions and a common network management model in a virtualized server environment. The Cisco Nexus 1000V Series Switch replaces the virtual switching functionality of the VMware vCenter data center container of servers. Each server in the data center container is represented as a line card in the Cisco Nexus 1000V Series Virtual Supervisor Module (VSM) and is managed as if it were a line card in a physical Cisco switch.

Key benefits of the Nexus 1000V include the following:

- Policy-based virtual machine (VM) connectivity
- Mobile VM security and network policy
- Non-disruptive operational model for your server virtualization, and networking teams

Table 5-24 PHI HIPAA Assessment Summary—Cisco Nexus 1000V Switch

Models Assessed
Cisco Nexus 1000V version 4.2(1)SV1(4)

Table 5-24 PHI HIPAA Assessment Summary—Cisco Nexus 1000V Switch

HIPAA Safeguards Addressed	
Administrative	**Standards/Implementation Specifications**
164.308	(a)(1)(i) Security Management Process
	(a)(3)(i) Authorization/Supervision
	(a)(4)(ii)(A) Isolating Healthcare Clearinghouse Functions
	(a)(4)(i) Access Authorization
	(a)(5)(i) Log-in Monitoring
	(a)(6)(i) Security Incident Procedures
Technical	**Standards/Implementation Specifications**
164.312	(a)(i) Access Control
	(b) Audit Controls
HIPAA Standards Failed	
No HIPAA standards were failed.	
HIPAA Implementation Specifications Failed	
No HIPAA implementation specifications were failed.	

Primary PHI Function

The primary HIPAA compliance feature of Cisco Nexus switches is secure aggregation and access layer connectivity.

- Using VLANs, Cisco Nexus switches allow an organization to put its ePHI network into separate VLANs (scopes) from other non-sensitive data (out of scope).
- The Layer 3 Cisco Nexus switch acts as a router, directing traffic between networks. By segmenting a network into sub-networks, an organization can isolate sensitive information from non-sensitive information. The Cisco Nexus switch can segment and route sensitive traffic separately from non-sensitive traffic to reduce the overall scope of a company's ePHI data environment. Depending on risk vectors, various levels of enforcement are required at the segmented scope boundary level.
- The Layer 3 Cisco Nexus switch acts as a router with ACLs, restricting traffic between the ePHI data environment and other areas of the network. A Cisco Nexus switch with ACLs can be used to enforce segmented traffic if the ACLs are used only to filter and segment private networks of the organization. ACLs may not be used to segment untrusted networks.
- The Cisco Nexus switch uses *virtualization contexts*, which are essentially virtualized switches. Each virtualized context has its own configuration and management interfaces that can be used to segregate not only data but administration as well.

Design Considerations

The Cisco Nexus 1000V Series Switch includes the Cisco Integrated Security features that are found on Cisco physical switches to prevent a variety of attack scenarios. For example, a rogue virtual machine can spoof its MAC and IP addresses so that it appears to be an existing production virtual machine, send a rogue Address Resolution Protocol (ARP) transaction mimicking the way that VMware vMotion announces the location of a migrated virtual machine, and divert traffic from the production virtual machine to the rogue virtual machine. With Cisco Integrated Security features, this type of attack can

easily be prevented with simple networking policy. Because server virtualization is being used for desktop and server workloads, it is critical that this type of security feature be deployed for the proper operation of a virtualized environment.

The Cisco Nexus 1000V Series implementation has two primary components:

- Virtual Supervisor Module (VSM)
- Virtual Ethernet module (VEM)

The Cisco Nexus 1000V VSM is installed as an appliance server on either a standalone Cisco UCS server (Cisco Nexus 1010) or as a virtual appliance on VMware ESXi server running on a blade of the Cisco UCS system.

HIPAA Assessment Detail—HIPAA Safeguards Addressed

All of the sample configurations of the Cisco Nexus 1000V Series Switch shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
- §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
- §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
- §164.308(a)(4)(ii)(A) Isolating healthcare clearinghouse function. If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
  - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
  - §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
  - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical Safeguards.
  - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. Requirements addressed include: Auditing.

Sample Configuration

Cisco Nexus 1000V is designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership.

To enable central authentication, you first have to enable the TACACS+ feature on the Cisco Nexus 1000V:

```
config t
feature tacacs+
```

The following commands show how to configure the TACACS+ server:

```
tacacs-server key 7 password
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
    use-vrf management
    source-interface mgmt0
aaa group server tacacs+ tacacs
aaa authentication login default group CiscoACS
aaa authentication login console group CiscoACS
```

Number *7* in the key command specifies an encrypted string (key) to follow.

Local individual user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration as specified in established policies for passwords. Configure the local user with encrypted passwords for fallback authentication:

```
username janoff password 5 <removed>  role network-admin
username bart password 5 <removed>  role network-operator
```

Both roles used in the **username** commands are pre-defined roles in the Cisco Nexus 1000V. The network admin role has access to all commands on the switch, whereas the network operator role has access to all read commands on the switch.

To address the Incident Response and Auditing HIPAA safeguards identified above, Cisco Nexus 1000V can be configured to send its log data to the RSA enVision log management platform. Cisco Nexus switches track individual administrator actions through several mechanisms including AAA, logging, and system events by implementing the following configuration statements:

```
logging server 192.178.42.124 6 facility syslog
aaa accounting default group CiscoACS
```

HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of automatic logoff options. Cisco Nexus 1000V supports session timeout, it is a best practice to set session timeout to 15 minutes, as shown below.

```
line vty
  exec-timeout 15
line console
  exec-timeout 15
```

NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The

Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. Cisco Nexus switches use NTP to meet these requirements by implementing the following configuration statements.

```
enable NTP
ntp server 192.168.62.161 use-vrf management
ntp server 192.168.62.162 use-vrf management
clock timezone PST -8 0
clock summer-time PST 1 Sun April 02:00 5 Sun Oct 02:00 60
```

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Cisco Nexus Switches—Data Center

The Cisco Nexus family of data center switches is designed to securely switch data from healthcare application servers to high speed trunks of the core, maintaining the integrity of segmented scopes of compliance. They provide scalable inter-switch connectivity and high port density for wired endpoints. VLANs are used to put sensitive applications and devices onto their own network and segregate them from devices on non-sensitive networks.

Cisco Nexus switches are ideal for enterprise-class server and aggregation layer deployments. These multipurpose, multilayer switches can be deployed across a diverse set of traditional, virtualized, unified, and high-performance computing environments. They enable diverse transports over Ethernet (including Layer 2, Layer 3, and storage traffic) on one common platform. Nexus switches help transform your data center, with a standards-based, multipurpose, multiprotocol, Ethernet-based fabric.

Table 5-25 PHI HIPAA Assessment Summary—Cisco Nexus Data Center Switches

Models Assessed	
Cisco Nexus5020 Chassis (“40x10GE/Supervisor”) version n5000-uk9.5.0.3.N1.1b.bin Cisco 7010 Chassis (“Supervisor module-1X”) version n7000-s1-dk9.5.1.2.bin	
HIPAA Safeguards Addressed	
Administrative	**Standards/Implementation Specifications**
164.308	(a)(1)(i) Security Management Process
	(a)(3)(i) Authorization/Supervision
	(a)(4)(ii)(A) Isolating Healthcare Clearinghouse Functions
	(a)(4)(i) Access Authorization
	(a)(5)(i) Log-in Monitoring
	(a)(6)(i) Security Incident Procedures
Technical	**Standards/Implementation Specifications**

Table 5-25 PHI HIPAA Assessment Summary—Cisco Nexus Data Center Switches

164.312	(a)(i) Access Control
	(b) Audit Controls
HIPAA Standards Failed	
No HIPAA standards were failed.	
HIPAA Implementation Specifications Failed	
No HIPAA implementation specifications were failed.	

Primary PHI Function

The primary HIPAA compliance feature of Cisco Nexus data center switches is secure aggregation and access layer connectivity.

- Using VLANs, Cisco Nexus switches allow an organization to put its ePHI network into separate VLANs (scopes) from other non-sensitive data (out of scope).
- The Layer 3 Cisco Nexus switch acts as a router, directing traffic between networks. By segmenting a network into sub-networks, an organization can isolate sensitive information from non-sensitive information. The Cisco Nexus switch can segment and route sensitive traffic separately from non-sensitive traffic to reduce the overall scope of a company's ePHI data environment. Depending on risk vectors, various levels of enforcement are required at the segmented scope boundary level.
- The Layer 3 Cisco Nexus switch acts as a router with ACLs, restricting traffic between the ePHI data environment and other areas of the network. A Cisco Nexus switch with ACLs can be used to enforce segmented traffic if the ACLs are used only to filter and segment private networks of the organization. ACLs may not be used to segment untrusted networks.
- The Cisco Nexus switch uses virtualization contexts, which are essentially virtualized switches. Each virtualized context has its own configuration and management interfaces that can be used to segregate not only data but administration as well.

Design Considerations

- Configuration was done manually on the router CLI, and backup of configuration and monitoring of configuration for changes and non-compliance were done through the Cisco Prime LMS (alternatively CiscoWorks Resource Manager Essentials, a component of C-LMS, can be used as well).
- Configure appropriate banner messages on login, incoming, and EXEC modes of the router. The login banner warning should not reveal the identity of the company that owns or manages the router. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Configure the primary login authentication of the router to be directed to the Cisco Secure ACS. Individual user account profiles need to be created. Configure secondary or tertiary authentication local to the router itself in the event of a WAN or Cisco Secure ACS failure.
- Nexus switches in the data center were implemented using guidance from the Enterprise Data Center Design guide based on a Data Center 3.0 Architecture:
  http://www.cisco.com/en/US/netsol/ns743/networking_solutions_program_home.html

  Enterprise Internet Edge Design Guide:
  http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/IE_DG.html

- The Cisco Nexus 7010 and the Cisco Nexus 5000 were used for the aggregation block portions of the lab validation network.

HIPAA Assessment Detail—HIPAA Safeguards Addressed.

All of the sample configurations of the Cisco Nexus data center switches shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
  - §164.308(a)(4)(ii)(A) Isolating healthcare clearinghouse function. If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
  - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
  - §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
  - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
  - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. Requirements addressed include: Auditing.

Sample Configuration

Cisco Nexus switches are designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership.

To enable central authentication, you first have to enable the TACACS+ feature on the Cisco Nexus 1000V:

```
config t
feature tacacs+
```

The following commands show how to configure the TACACS+ server:

```
tacacs-server key 7 "<removed>"
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
    use-vrf management
    source-interface mgmt0
aaa group server tacacs+ tacacs
aaa authentication login default group CiscoACS
aaa authentication login console group CiscoACS
```

Number *7* in the key command specifies an encrypted string (key) to follow.

Local individual user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration as specified in established policies for passwords. Configure the local user with encrypted passwords for fallback authentication:

```
username janoff password 5 <removed>  role network-admin
username bart password 5 <removed>  role network-operator
```

Both roles used in the **username** commands are pre-defined roles in the Cisco Nexus 1000V. The network admin role has access to all commands on the switch, whereas the network operator role has access to all read commands on the switch.

To address the Incident Response and Auditing HIPAA Safeguards identified above, Cisco Nexus 1000v can be configured to send its log data to the RSA enVision log management platform. Cisco Nexus switches track individual administrator actions through several mechanisms including AAA, logging, and system events by implementing the following configuration statements:

```
logging server 192.178.42.124 6 facility syslog
!
! --- for implementations using VRF's ----
!
logging server 192.168.42.124 6 use-vrf servers1

aaa accounting default group CiscoACS
```

HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of automatic logoff options. Cisco Nexus 1000V supports session timeout, it is a best practice to set session time-out to 15 minutes, as shown below.

```
line vty
  exec-timeout 15
line console
  exec-timeout 15
```

NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. Cisco Nexus switches use NTP to meet these requirements by implementing the following configuration statements.

```
! NTP can only be configured in the default VDC
!
```

```
enable NTP
ntp server 192.168.62.161 use-vrf management
ntp server 192.168.62.162 use-vrf management
clock timezone PST -8 0
clock summer-time PST 1 Sun April 02:00 5 Sun Oct 02:00 60
```

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Wireless

Cisco Wireless technologies provide connectivity for mobile clients within the clinic. They are designed to securely connect traditional business functions such as guest access, without increasing risk. In addition to expanding business functionality, Cisco wireless technology seamlessly provides the capability to detect rogues.

Cisco Aironet access points are designed to provide industry-leading performance to enable highly secure and reliable wireless connections for both indoor and outdoor environments. Cisco offers a broad portfolio of access points targeted to specific business needs and topologies.

Cisco wireless controllers help reduce the overall operational expenses of Cisco Unified Wireless Networks by simplifying network deployment, operations, and management. They extend policy and security from the wired network to the wireless edge.

Cisco Wireless Control System (WCS) delivers full visibility and control of Cisco Aironet access points, Cisco Wireless LAN Controllers (WLC) and the Cisco Mobility Services Engine (MSE) with built-in support for Cisco adaptive wireless intrusion prevention systems (wIPS) and Cisco context-aware services. This robust platform helps you reduce total cost of ownership and maintain a business-ready wireless network.

Table 5-26 PHI HIPAA Assessment Summary—Cisco Wireless Products

Models Assessed	
AIR-CT5508-12-K9 version 7.0.114.112 MSE3550 version 7.0.200.125 Cisco WCS Manager version 7.0.171.107 AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N	
HIPAA Safeguards Addressed	
Administrative	**Standards/Implementation Specifications**
164.308	(a)(1)(i) Security Management Process
	(a)(3)(i) Authorization/Supervision

Table 5-26 PHI HIPAA Assessment Summary—Cisco Wireless Products (continued)

	(a)(4)(i) Access Authorization
	(a)(5)(i) Log-in Monitoring
	(a)(6)(i) Security Incident Procedures
	(a)(6)(i) Response and Reporting
Technical	**Standards/Implementation Specifications**
164.312	(a)(i) Access Control
	(a)(2)(i) Unique User Identification
	(a)(2)(ii) Emergency Access procedures
	(a)(2)(ii) Automatic Logoff
	(a)(ii)(iv) Encryption and Decryption
	(b) Audit Controls
	(c)(1) Data Integrity
	(d) Person or Entity Authentication
	(e)(i) Transmission Security
	(e)(2)(i) Integrity Controls
	(e)(2)(ii) Encryption
HIPAA Standards Failed	
No HIPAA standards were failed.	
HIPAA Implementation Specifications Failed	
No HIPAA implementation specifications were failed.	

Primary PHI Function

The primary ePHI function of Cisco Unified Wireless is secure connectivity and authentication of wireless clients as well as rogue device detection.

Design Considerations

Wireless technology in the PHI environment is a growing concern for organizations in the healthcare field. Implementing wireless requires that appropriate security controls are in place to prevent, detect and respond to security violations. A hacker might infiltrate a PHI environment and install a rogue wireless device (for example, access point, wireless-enabled printer, or radio-enabled USB stick). This would allow a hacker remote access into the PHI environment (from the parking lot, for example) that is hard to detect. There are several methods for detecting rogue devices. Cisco Unified Wireless offers the benefit of continuous rogue detection while simultaneously passing normal wireless traffic.

Wireless technology is an untrusted network connection. Appropriate security must be is in place for wireless technology in the ePHI environment. Organizations must ensure that controls are in place to prevent unauthorized access. Appropriate controls include a firewall to segment and protect the PHI data environment and intrusion detection services to identify potential intrusion attempts to the secured network. Stateful firewalls must be configured to limit traffic to and from the wireless environment (all enabled services, protocols, and ports must have documented justification for business purposes). All other access should be denied.

When implementing wireless in an ePHI environment, encryption must be configured to adequately protect ePHI transmitted over the wireless medium. Today the minimum level of encryption deemed acceptable by auditors is WPA2.

Cisco recommends using the Unified Wireless (controller-based) architecture for enterprise wireless deployments because of the Cisco ongoing wireless strategy. The autonomous Cisco IOS access points are not being enhanced. Future security and user enhancements will be developed on the controller-based architecture.

For WCS servers running software versions prior to 4.1, Cisco recommends a combination of documented password policies, manual audit procedures, and firewall segmentation for WCS servers within the data center.

- Configure unique SSIDs
- Disable broadcast of the SSIDs

HIPAA Assessment Detail—HIPAA Safeguards Addressed

All of the sample configurations of the Cisco Wireless technologies shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.308(a)(4)(ii)(A) Isolating healthcare clearinghouse function. If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
  - §164.308(a)(4)(ii)(C) Access Establishment and Modification. Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. Requirements addressed include: Access Control, Incident Response, and Auditing.
  - §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).
  - §164.312(d) Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. Requirements addressed include: Access Control and Auditing.
  - §164.308(a)(5)(ii)(D) Password Management. Procedures for creating, changing, and safeguarding passwords. Requirements addressed include: Access Control and Auditing.
- Integrity—Protect electronic protected health information from improper alteration or destruction as required by HIPAA Technical safeguards.

  - §164.312(c)(1) Data Integrity. Implement policies and procedures to protect health information from improper alteration or destruction.
  - §164.308(a)(4)(ii)(C) Access Establishment and Modification. Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. Requirements addressed include: Access Control, Incident Response, and Auditing.
  - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
  - §164.312(a)(2)(ii) Emergency Access Procedure. Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.
  - §164.312(e)(1) Transmission Security. Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network. Requirements addressed include: Encryption and Integrity.
  - §164.308(e)(2)(i) Integrity Controls. Implement security measures to ensure that ePHI is not improperly modified without detection until disposed of. Requirements addressed include: Integrity.
  - §164.308(e)(2)(ii) Encryption. Implement a mechanism to encrypt ePHI whenever deemed appropriate. Requirements addressed include: Encryption.

- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
  - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
  - §164.312(a)(2)(i) Unique User Identification. Assign a unique name and/or number for identifying and tracking user identity. Requirements addressed include: Access Control and Auditing.
  - §164.312(a)(2)(ii) Automatic logoff. Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. Requirements addressed include: Access Control and Auditing.
- Encryption—Implement mechanisms to encrypt and decrypt ePHI.
  - §164.312(a)(ii)(iv) Encryption and Decryption. Implement a mechanism to encrypt and decrypt electronic protected health information. Requirements addressed include: Encryption and Integrity.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
  - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. Requirements addressed include: Auditing.
  - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
  - §164.312(d) Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. Requirements addressed include: Access Control and Auditing.

Sample Configuration

Cisco WCS is designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership.

Cisco Unified Wireless allows the network administrator to set user IDs that can be monitored and restricted with respect to access and other privileges when necessary.

For network security, the Cisco solution uses profiles for appropriate access where a user is assigned to the profile, and user access can be restricted as shown in Figure 5-101 and Figure 5-102.

Figure 5-101 Local Management Users Screen

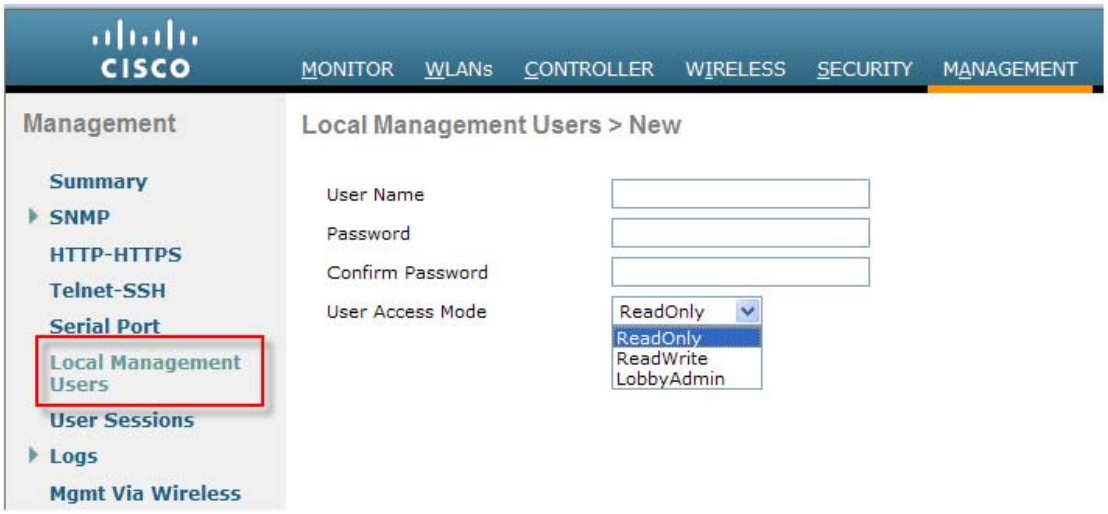
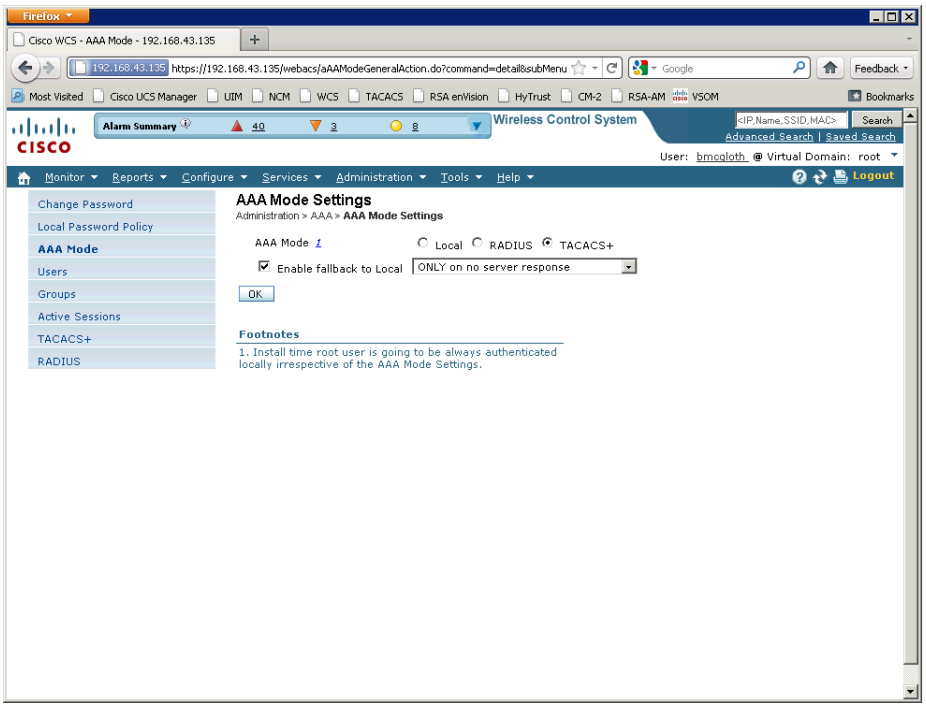


Figure 5-102 Management Via Wireless Screen

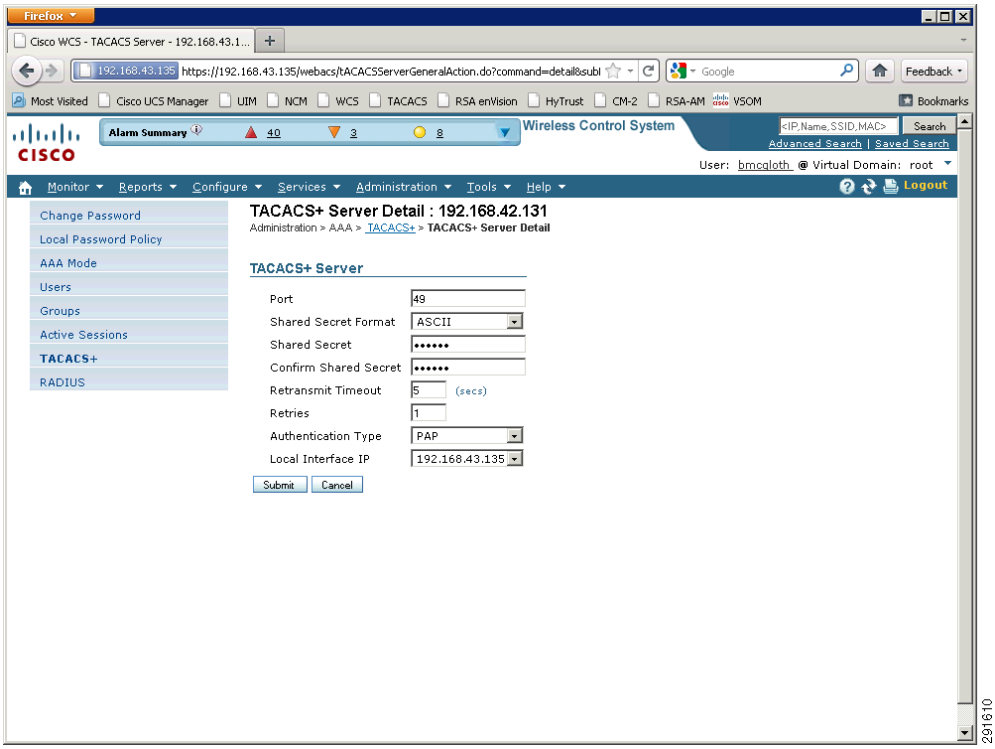
Cisco WCS is configured to use TACACS+ for authentication of administrators, as shown in Figure 5-103.

Figure 5-103 WCS Manager AAA Authentication Mode



The authentication servers for TACACS+ in WCS Manager are configured as shown in Figure 5-104.

Figure 5-104 WCS Manager TACACS+ Server Configuration

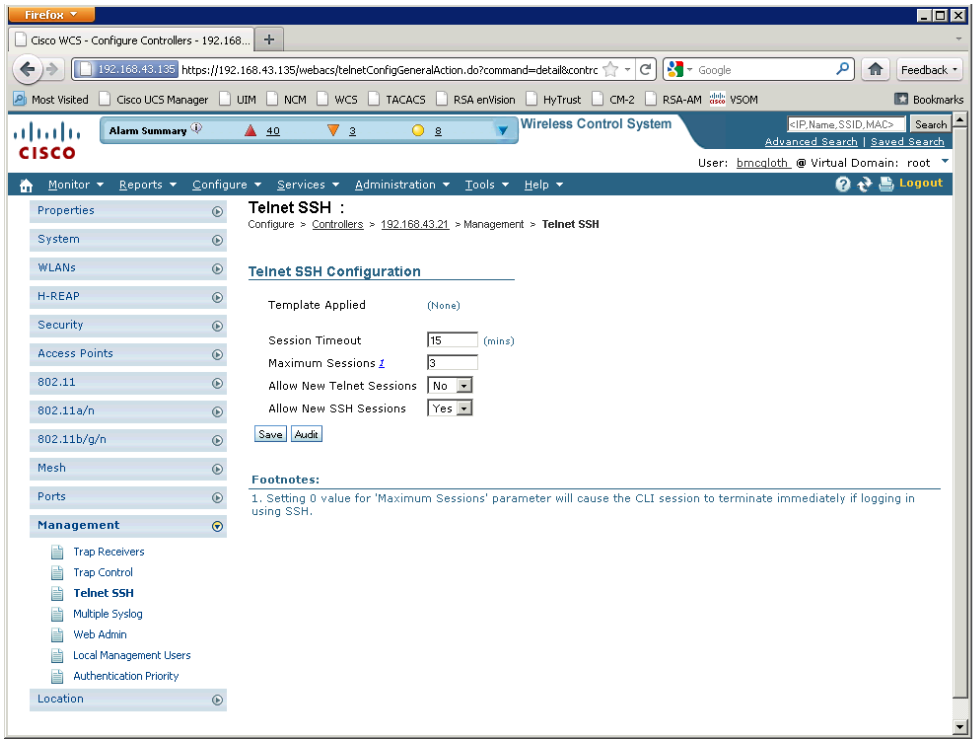


The citations in this section were addressed with the sample configuration at the end of this section.

Local individual user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration as specified in established policies for passwords. Local user accounts on Cisco WCS Manager and controllers require a password.

HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of Automatic logoff options. Cisco WCS supports session policies under the management tab. It is a best practice to change the session timeout to 15 minutes, as shown in Figure 5-105.

Figure 5-105 Controller Secure Management for SSH



The Cisco WLAN performs 24-hour scanning to immediately detect and contain unauthorized and rogue wireless devices addressing safeguard 164.308(a)(1)(i) Security Management. Threats to network security can occur in between regularly scheduled scans, creating the need to continuously scan and to use automatic alerts and containment mechanisms. Similarly, physical and/or port scanning on the wired network is not enough. Cisco Wireless LAN Controllers include wIPS and wIDS that find and stop rogue wireless devices and attacks. WCS is a single point of management for WLAN devices, the mobility services engine, and mobility services. Cisco context-aware location services in the Cisco 3300 Series Mobility Services Engine (MSE) can locate multiple rogue devices. Cisco enhanced local mode (ELM) access points offer monitor mode wIPS on local mode access points for additional protection without a separate overlay network. Cisco CleanAir technology allows the detection and location of rogue devices on nonstandard Wi-Fi channels. (See Figure 5-106 and Figure 5-107.)

Figure 5-106 Security—AP Policies Screen

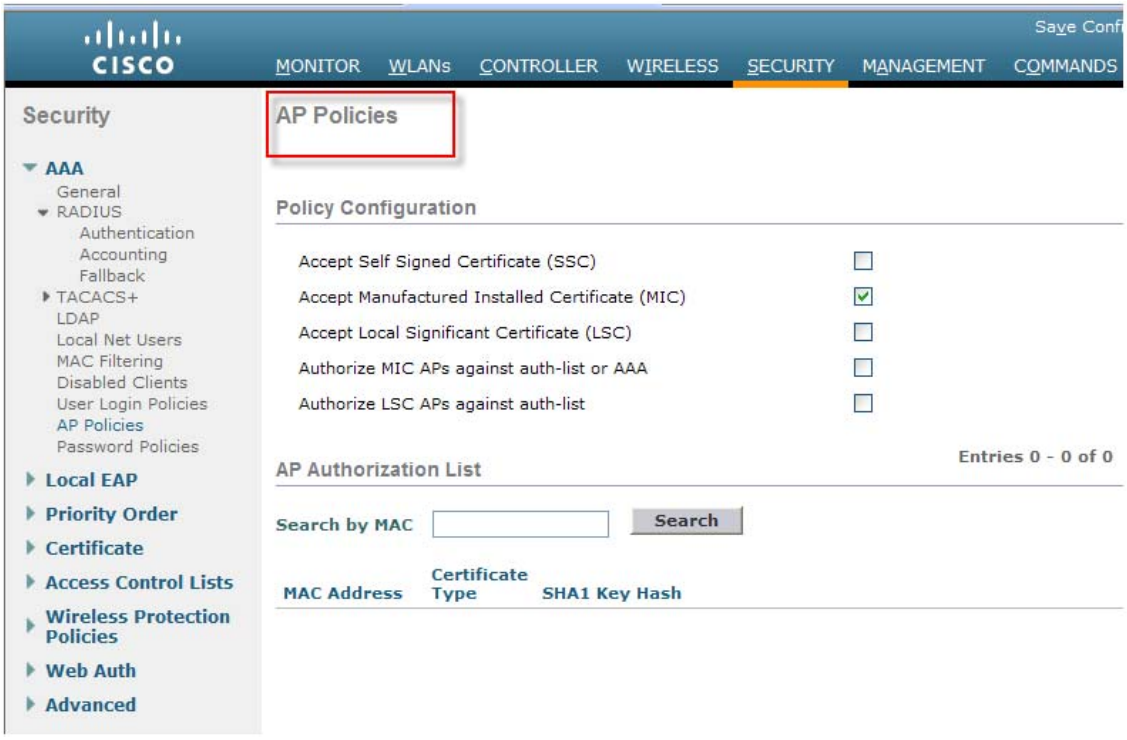
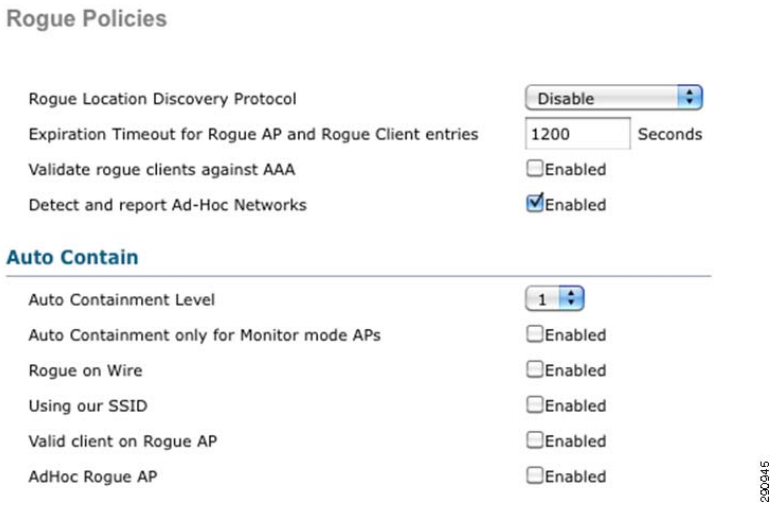
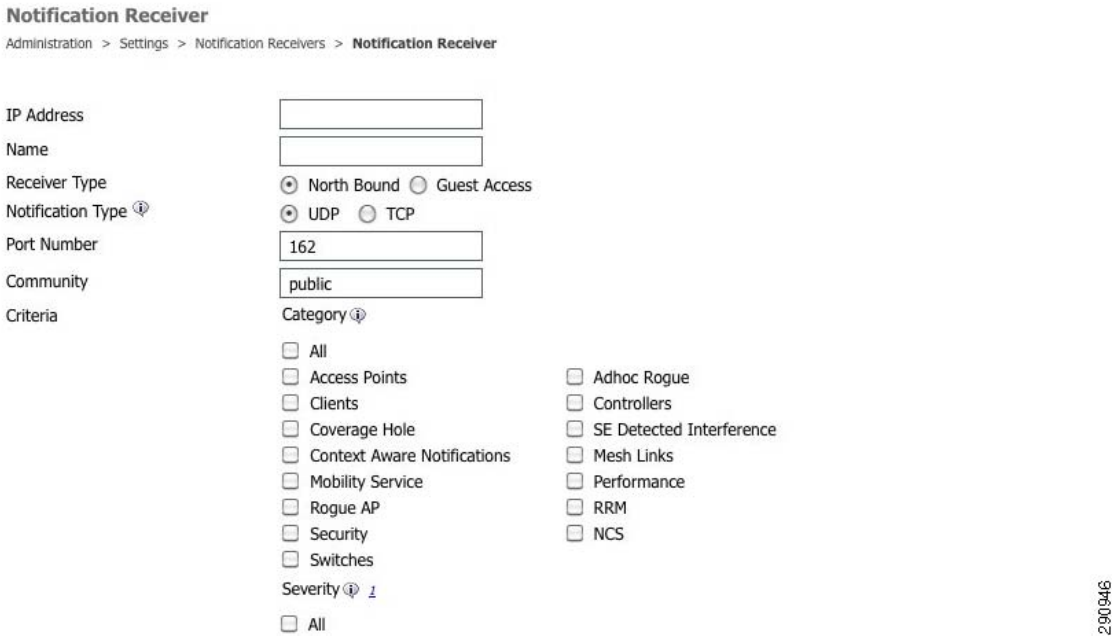


Figure 5-107 Rogue Policies Screen



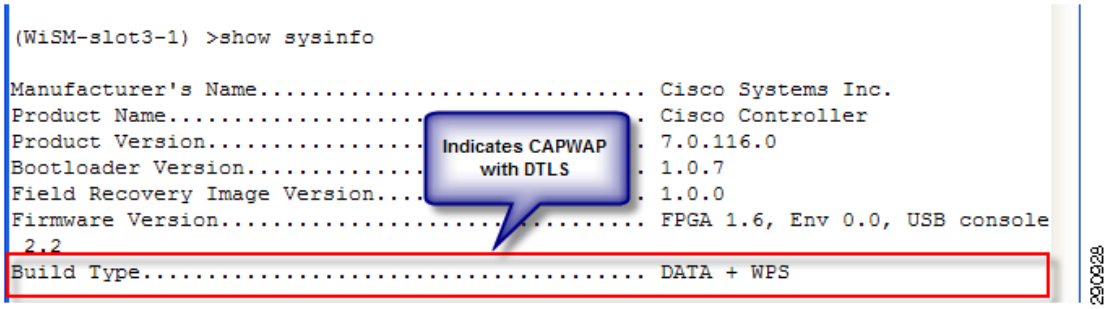
Cisco WCS has the ability to forward alerts to e-mail addresses. The system can forward all or selected alerts to multiple receivers. (See Figure 5-108.)

Figure 5-108 Notification Receiver Screen



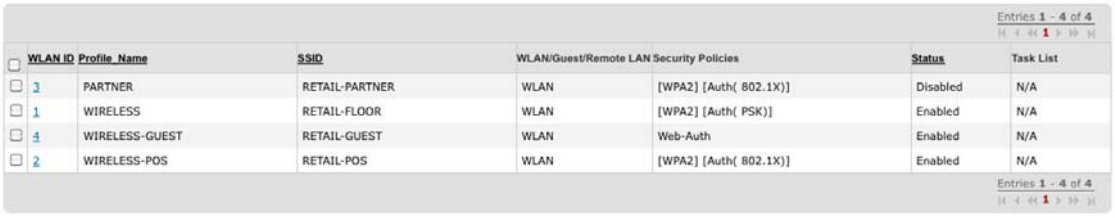
Cisco offers Control and Provisioning of Wireless Access Points (CAPWAP)-compliant DTLS encryption to provide full-line-rate encryption between access points and controllers across remote WAN/LAN links (see Figure 5-109). The Cisco Unified Wireless Network defaults to the highest CipherSuite available on the network. Furthermore, fallback on less secure SSL versions (that is, SSLv2 and SSLv1) can also be disabled, thus always forcing use of SSLv3. The Cisco Unified Wireless Network provides 256-bit encryption and provides automated vulnerability scanning in the WCS to identify WLANs using suboptimal encryption/authentication configurations.

Figure 5-109 CAPWAP with DTLS



Cisco supports both WPA and WPA2 and provides automated vulnerability scanning in the WCS to identify WLANs using suboptimal encryption. Cisco does not advertise the organization's name in the Service Set ID (SSID) broadcast. Cisco also disables SSID broadcast by default for non-guest networks. Cisco supports WPA2 Personal mode with a minimum 13-character random pass-phrase and Advanced Encryption Standard (AES) encryption, and provides automated vulnerability scanning in the WCS to identify WLANs using suboptimal encryption/authentication configurations. (See Figure 5-110.)

Figure 5-110 WLAN Information



The citations in this section were addressed with the sample configuration at the end of this section.

To address the Incident Response and Auditing HIPAA Safeguards identified above, the Cisco Unified Wireless system is designed to track and monitor all administrative user access and events. Cisco Unified Wireless tracks individual administrator actions through several mechanisms including AAA, logging, and system events.

Figure 5-111 shows the configuration of local logging settings, and Figure 5-112 shows the syslog server configuration used to send logs to RSA enVision.

Figure 5-111 Local Logging Configuration

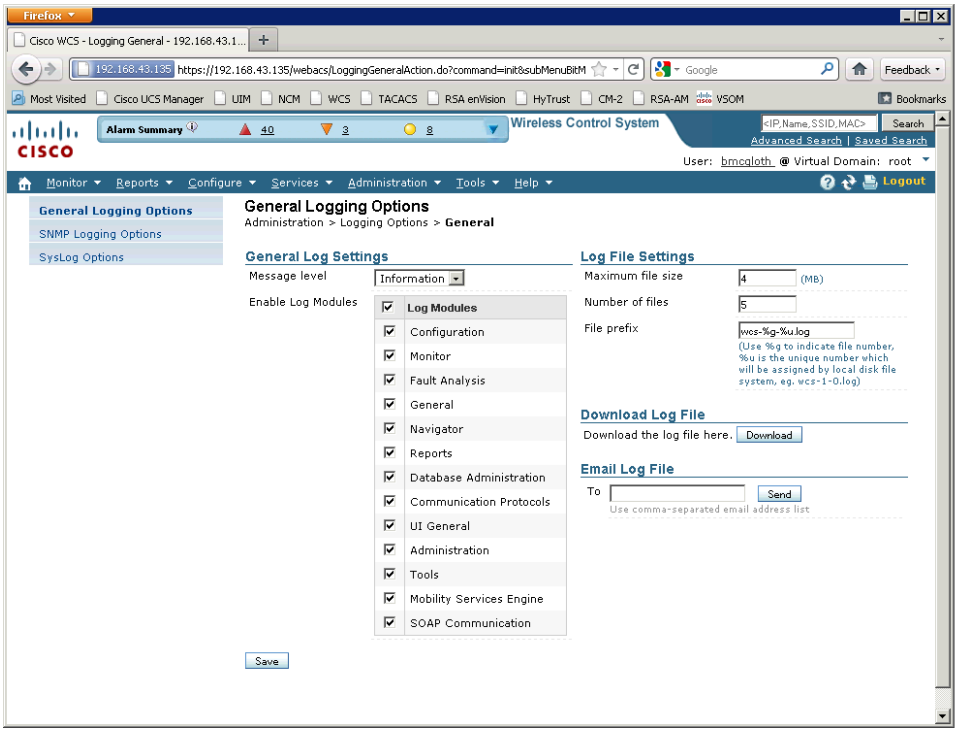
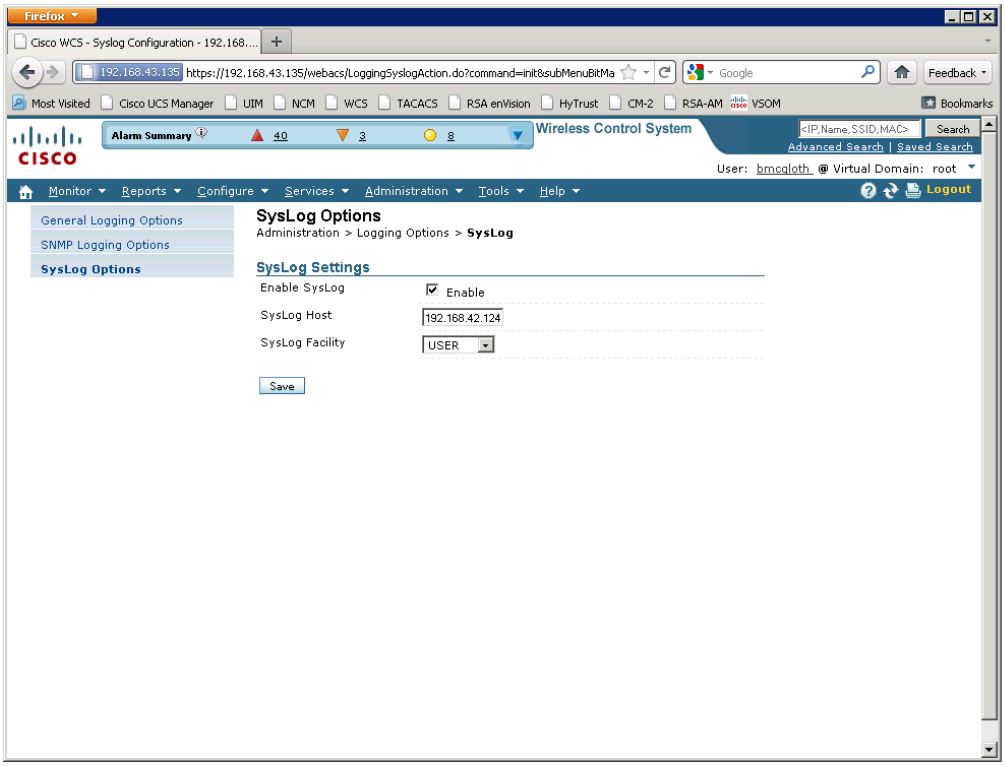


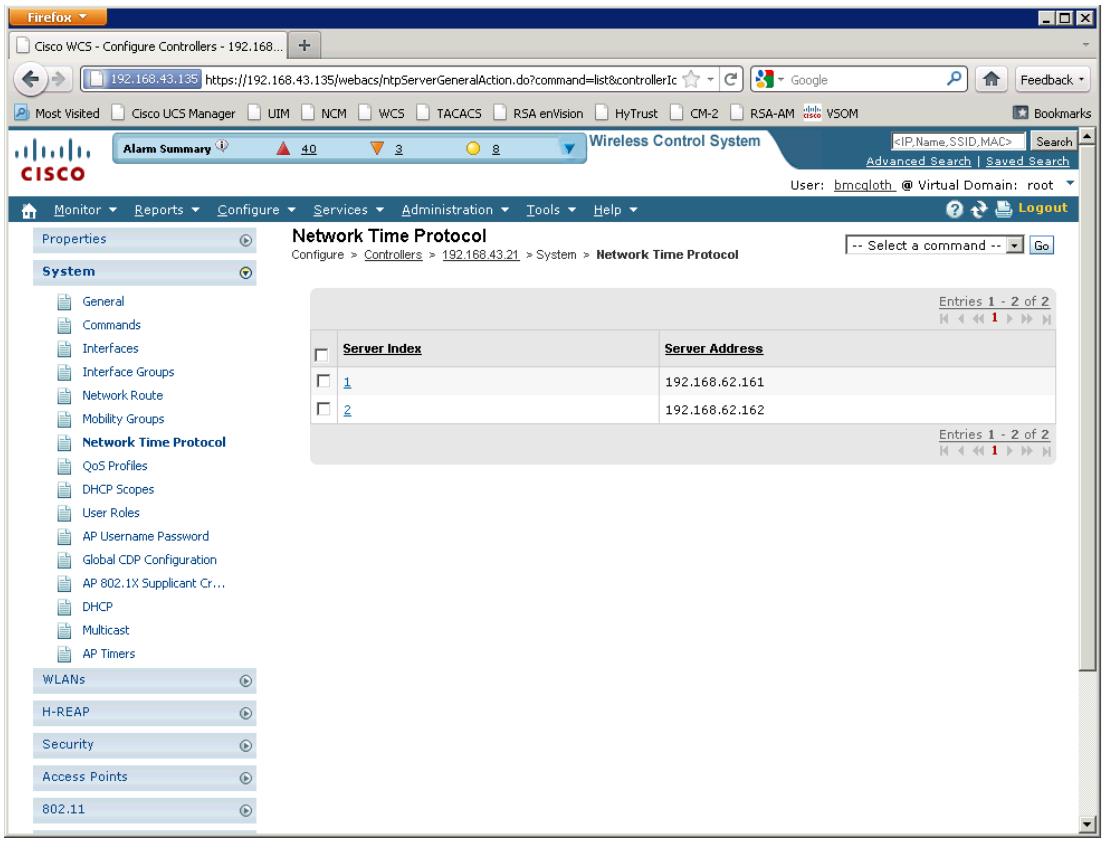
Figure 5-112 WCS Manager Syslog Configuration



As a best practice, NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

A Network Time Protocol server can be configured within the Cisco WCS and Controllers to meet this requirement for all wireless devices, as shown in Figure 5-113.

Figure 5-113 NTP Servers Screen for Controllers



HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Storage

Cisco MDS Storage Switches

Cisco MDS storage switches provide the central switching infrastructure connecting servers to storage. They provide the added capability to encrypt all information “on the fly” between these systems for specified targets; specifically, the EMC storage array and Cisco UCS servers in the solution.

The Cisco MDS 9000 Series Multilayer SAN Switches can help lower the total cost of ownership of the most demanding storage environments. By combining robust and flexible hardware architecture with multiple layers of network and storage management intelligence, the Cisco MDS 9000 Series helps you build highly available, scalable storage networks with advanced security and unified management.

Table 5-27 PHI HIPAA Assessment Summary—Cisco MDS Storage Switches

Models Assessed	
MDS 9506 (“Supervisor/Fabric-2”) version m9500-sf2ek9-mzg.5.0.1a.bin.S4 MDS 9506 (“Supervisor/Fabric-2”) version m9500-sf2ek9-mz.5.0.4.bin	
HIPAA Safeguards Addressed	
Administrative	**Standards/Implementation Specifications**
164.308	(a)(1)(i) Security Management Process
	(a)(4)(i) Access Authorization
	(a)(5)(i) Log-in Monitoring
	(a)(6)(i) Security Incident Procedures
Technical	**Standards/Implementation Specifications**
164.312	(a)(i) Access Control
	(a)(2)(iv) Encryption and Decryption
	(b) Audit Controls
	(c)(1) Data Integrity
HIPAA Standards Failed	
No HIPAA standards were failed.	
HIPAA Implementation Specifications Failed	
No HIPAA implementation specifications were failed.	

Primary PHI Function

The primary function of Cisco MDS storage switches is to securely encrypt ePHI data at rest as it passes from server to storage. This safeguard was met using the MDS configuration to implement encryption for ePHI data in storage to prevent unauthorized access and prevent unauthorized modification to the ePHI data. Logs can be used to monitor access attempts to ePHI data in storage.

Design Considerations

Cisco MDS 9000 Family security features such as VSANs, advanced zoning, fabric binding, port security, Fiber Channel Security Protocol (FC-SP) authentication, and role-based access control (RBAC) with SNMPv3 and SSH make the Cisco MDS 9000 Family an excellent platform for enforcing this requirement. SSH RBAC in particular, if used in conjunction with VSANs, is especially designed to support tight partitioning of the physical infrastructure.

The MDS 9500s were configured for zoning and LUN masking to secure the logical partitioning of disk used for storing ePHI data. Only host machines in the data center that require access to that logical disk partition were allowed access. Configuration of the VSANs, host UUIDs, and mappings was partially performed using EMC Unified Infrastructure Manager as directed by the Vblock architecture by VCE. Vblock requires specific software versions and pre-configurations to be completed as specified in the Vblock preparation guide.

More information of Vblock designs can be found at the following URL:
http://www.vceportal.com/solutions/68580567.html#

Information in installing and configuring Cisco MDS can be found at the following URL:
http://www.cisco.com/en/US/products/hw/ps4159/ps4358/tsd_products_support_series_home.html

HIPAA Assessment Detail—HIPAA Safeguards Passed

All of the sample configurations of the Cisco MDS storage switches shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
  - §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
  - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
  - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
  - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. Requirements addressed include: Auditing.
- Integrity—Protect electronic protected health information from improper alteration or destruction as required by HIPAA Technical safeguards.
  - §164.312(c)(1) Data Integrity. Implement policies and procedures to protect health information from improper alteration or destruction.

Sample Configuration

Cisco MDS storage switches are designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership.

The following configurations demonstrate how to configure the Cisco MDS for TACACS+ authentication to a central server.

```
Feature tacacs+

tacacs-server key 7 "<removed>"
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
```

```
    server 192.168.42.131

aaa authentication login default group CiscoACS
aaa authentication login console group CiscoACS
aaa authorization ssh-certificate default group CiscoACS
aaa accounting default group CiscoACS
aaa authentication login error-enable
```

Note To configure LDAP authentication in NX-OS version 5.0 or higher, enable LDAP (**feature ldap**) and follow configuration steps in the *Cisco MDS 9000 Family NX-OS Security Configuration Guide.*

Assignment of privileges to individuals based on job classification and function is accomplished with the following configuration:

```
Feature privilege
        change admin user ID:
        username admin password <password> role network-admin (password will be
encrypted when displayed)
        create network operator type user ID:
        username <assigned name> password <password> role network-operator (password
will be encrypted when displayed)
        create default user ID:
        role name default-role
            description This is a system defined role and applies to all users.
            rule 5 permit show feature environment
            rule 4 permit show feature hardware
            rule 3 permit show feature module
            rule 2 permit show feature snmp
            rule 1 permit show feature system
        username <assigned name> password <password> role default-role (password will
be encrypted when displayed)
        create custom user ID:
        role name <name>
            description User defined permissions define here:
            rule 1 permit show interface
            .
            .
            Rune 256 permit show module
        username <assigned name> password <password> role <name> (password will be
encrypted when displayed)
```

Local individual user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration as specified in established policies for passwords.

```
username bmcgloth password 5 <removed>   role network-admin
username bart password 5 <removed>   role network-admin
```

HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of automatic logoff options. Cisco MDS supports session timeout configuration in the CLI. It is a best practice to set the session timeout to 15 minutes, as shown below.

```
line vty
  exec-timeout 15
line console
  exec-timeout 15
```

To secure authentication information and management of the Cisco MDS Switch, addressing Safeguard 164.308(a)(1)(i) Security Management, the management intercedes are configured to support only encrypted access using the following configurations:

```
Configure terminal
feature ssh
ssh key dsa or ssh key rsa <768-2048>
no feature telnet
no feature http-server
```

And access to the management interface is restricted with an access list.

Secure access to the management port as follows:

```
ip access-list 23 permit ip 127.0.0.1 0.0.0.0 <mgmt port ip address> 0.0.0.0
ip access-list 23 permit ip <ip address of mgmt workstation> 0.0.0.0 <mgmt port ip
address> 0.0.0.0
ip access-list 23 permit ip <ip address of snmp workstation> 0.0.0.0 <mgmt port ip
address> 0.0.0.0
ip access-list 23 permit ip <ip address of AAA server> 0.0.0.0 <mgmt port ip address>
0.0.0.0
ip access-list 23 permit ip <ip address of NTP workstation> 0.0.0.0 <mgmt port ip
address> 0.0.0.0
ip access-list 23 deny ip any any log-deny
interface mgmt0
ip address <ip address> <mask>
ip access-group 23 in
```

To address the Incident Response and Auditing HIPAA safeguards identified above, the Cisco MDS 9000 Family implements the Cisco Data Center Network Manager (DCNM), which continuously monitors the SAN and allows you to establish criteria and thresholds to generate real-time alarms and call-home functions. Syslog and SNMP traps offers detailed entries and can be redirected to the RSA enVision log server to consolidate IT infrastructure monitoring information. Note that the log never contains application data. Cisco MDS is designed to track and monitor all administrative user access and events.

Logs stored locally are buffered and require operator level privileges to be viewed. External logging and SNMP traps are enabled by implementing the following configuration statements:

```
logging server 192.168.42.124 6
snmp-server host 192.168.41.101 traps version 2c public  udp-port 2162
snmp-server host 192.168.42.121 traps version 3 auth public
```

A central logging repository, RSA enVision, collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

As a best practice, NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. Cisco MDS use NTP to meet these requirements by implementing the following configuration statements:

```
clock timezone PST -8 0
clock summer-time PST 1 Sun April 02:00 5 Sun Oct 02:00 60
ntp server 192.168.62.161
ntp server 192.168.62.162
```

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Security

Cisco ASA Firewalls

The Cisco Adaptive Security Appliance (ASA) is designed to provide secure segmentation within a network. The stateful firewall and modular intrusion detection modules enable the healthcare entity to securely connect public networks to the PHI environment. The ASA also enables secure connectivity from remote locations via encrypted tunnels using its VPN technology.

The Cisco ASA delivers superior scalability, a broad span of technology and solutions, and effective, always-on security designed to meet the needs of a wide array of deployments. By integrating the world's most proven firewall; a comprehensive, highly effective intrusion prevention system (IPS) with Cisco Global Correlation and guaranteed coverage; high-performance VPN and always-on remote access, the Cisco ASA helps organizations provide secure, high performance connectivity and protects critical assets for maximum productivity.

The Cisco ASA 5500 Series includes the Cisco ASA 5505, 5510, 5512-X, 5515-X, 5520, 5525-X, 5540, 5545-X, 5550, 5555-X, 5580, and 5585-X Adaptive Security Appliances-purpose-built, high-performance security solutions that take advantage of Cisco expertise in developing industry-leading, award-winning security and VPN solutions. Through Cisco Multi-Processor Forwarding (MPF), the Cisco ASA 5500 Series brings a new level of security and policy control to applications and networks. MPF enables highly customizable, flow-specific security policies that have been tailored to application requirements. The performance and extensibility of the Cisco ASA 5500 Series is enhanced through user-installable security service modules (SSMs) and virtual modules. This adaptable architecture enables businesses to rapidly deploy security services when and where they are needed, such as tailoring inspection techniques to specific application and user needs or adding additional intrusion prevention and content security services such as those delivered by the Adaptive Inspection and Prevention (AIP) and Content Security and Control (CSC) SSMs. Furthermore, the modular hardware architecture of the Cisco ASA 5500 Series, along with the powerful MPF, provides the flexibility to meet future network and security requirements, extending the investment protection provided by the Cisco ASA 5500 Series and allowing businesses to adapt their network defenses to new threats as they arise.

The Cisco ASA Services Module (ASASM) is an integrated module installed inside a Cisco Catalyst 6500 Series Switch or Cisco 7600 Internet Router. The Cisco ASASM allows any port on the Cisco Catalyst switch to operate as a firewall port and integrates firewall security inside the network infrastructure.

All Cisco ASA offer both IPsec and SSL/DTLS VPN solutions; Clientless and AnyConnect VPN features are licensed at various price points, on a per-seat and per-feature basis. By converging SSL and IPsec VPN services with comprehensive threat defense technologies, the Cisco ASA provides highly customizable, granular network access tailored to meet the requirements of diverse deployment environments, while providing advanced endpoint and network-level security.

Table 5-28 PHI HIPAA Assessment Summary—Cisco ASA

Models Assessed	
Cisco ASA5515-X w/vIPS Module version asa900-129-smp-k8.bin and IDS version 7.1(6)	
Cisco ASA5555-X w/vIPS module version asa900-129-smp-k8.bin and IPS version 7.1(6)E4	
Cisco ASA5585-S60-2A-K9 asa901-smp-k8.bin	
Cisco ASA Service Module WS-SVC-ASA-SM1 version asa851-smp-k8.bin	
HIPAA Safeguards Addressed	
Administrative	**Standards/Implementation Specifications**
164.308	(a)(1)(i) Security Management Process
	(a)(1)(ii)(D) Information System Activity Review
	(a)(3)(ii)(A) Authorization/Supervision
	(a)(4)(ii)(A) Isolating Healthcare Clearinghouse Function
	(a)(4)(ii)(B) Access Authorization
	(a)(4)(ii)(C) Access Est./Modification
	(a)(5)(ii)(C) Log-in Monitoring
	(a)(6)(ii) Response and Reporting
Technical	**Standards/Implementation Specifications**
164.312	(a)(1) Access Control
	(a)(2)(i) Unique User Identification
	(a)(2)(ii) Emergency Access procedures
	(a)(2)(ii) Automatic Logoff
	(a)(ii)(iv) Encryption and Decryption
	(b) Audit Controls
	(c)(1) Data Integrity
	(d) Person or Entity Authentication
	(e)(1) Transmission Security
	(e)(2)(i) Integrity Controls
	(e)(2)(ii) Encryption
HIPAA Standards Failed	
No HIPAA standards were failed.	
HIPAA Implementation Specifications Failed	
No HIPAA implementation specifications were failed.	

Primary PHI Function

The primary function of the Cisco ASA firewall in a healthcare network environment is to securely segment PHI data environments to prevent unauthorized access from public and business associate networks at clinics, hospitals, clearinghouses and to provide intrusion detection capabilities. Additionally, the firewall can provide the isolation necessary for organizations with clearing house functions to protect against unauthorized access to the clearing house from the larger organization.

Design Considerations

- Select the appropriate Cisco ASA model/SSM module for the traffic needs in the healthcare entity.
- Configure security policies, objects, and rules centrally with Cisco Security Manager to support segmentation of the LAN from Internet exposure, implement restrictions based on identity and authorization to access ePHI, and set up logging and monitoring alerts for central capture and auditing.
- Firewall rule sets must adhere to a "least amount of access necessary" policy. Rules must be defined by specific source/destination addressing and TCP/UDP ports.
- Allow only SSHv2 (and not Telnet or SSHv1) connection from network management station to Cisco ASA.
- Configure appropriate banner messages on login, incoming, and exec modes of the Cisco ASA. The login banner warning should not reveal the identity of the company that owns or manages the Cisco ASA. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Configure the primary login authentication of the Cisco ASA to be directed to the Cisco Secure ACS. Individual user account profiles need to be created. Configure secondary or tertiary authentication local to the Cisco ASA itself in the event of connectivity or Cisco Secure ACS failure.
- Change default passwords and community strings to appropriate complexity.
- Configure the **ip verify reverse path** command on all interfaces to provide anti-spoofing functionality.
- Configure the console timeout commands to 15 minutes or less on the console of the Cisco ASA.
- For Internet edge, disable **icmp permit** on the outside interface of Cisco ASA. If users need to access servers in the DMZ segment, make sure that external users can reach the servers using very specific protocol and ports.

HIPAA Assessment Detail—HIPAA Safeguards Addressed

HIPAA safeguards are spread across multiple categories. The ASA firewall helps healthcare-covered entities and business associates meet access control safeguards in the Administrative and Technical categories. The access control can be applied to both internal and external users that access ePHI data. Additionally, controls to protect the administrator accounts on the firewall have been implemented to protect the firewall from unauthorized modification if the authentication server fails. These local accounts represent only a subset of select individuals that would need access in the event central authentications services are unavailable.

All of the sample configurations of the ASA shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
  - 164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - 164.308(a)(4)(ii)(A) Isolating healthcare clearinghouse function. If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.

  - 164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
  - 164.308(a)(4)(ii)(C) Access Establishment and Modification. Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. Requirements addressed include: Access Control, Incident Response, and Auditing.
  - 164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4).
  - 164.312(d) Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. Requirements addressed include: Access Control and Auditing.
  - 164.308(a)(5)(ii)(D) Password Management. Procedures for creating, changing, and safeguarding passwords. Requirements addressed include: Access Control and Auditing.
- Integrity—Protect electronic protected health information from improper alteration or destruction as required by HIPAA Technical safeguards.
  - 164.312(c)(1) Data Integrity. Implement policies and procedures to protect health information from improper alteration or destruction.
  - 164.308(a)(4)(ii)(C) Access Establishment and Modification. Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. Requirements addressed include: Access Control, Incident Response, and Auditing.
  - 164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
  - 164.312(a)(2)(ii) Emergency Access Procedure. Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.
  - 164.312(e)(1) Transmission Security. Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network. Requirements addressed include: Encryption and Integrity.
  - 164.308(e)(2)(i) Integrity Controls. Implement security measures to ensure that ePHI is not improperly modified without detection until disposed of. Requirements addressed include: Integrity.
  - 164.308(e)(2)(ii) Encryption. Implement a mechanism to encrypt ePHI whenever deemed appropriate. Requirements addressed include: Encryption.
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
  - 164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
  - 164.312(a)(2)(i) Unique User Identification. Assign a unique name and/or number for identifying and tracking user identity. Requirements addressed include: Access Control and Auditing.

  - 164.312(a)(2)(ii) Automatic logoff. Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. Requirements addressed include: Access Control and Auditing.

- Encryption—Implement mechanisms to encrypt and decrypt ePHI.
  - 164.312(a)(ii)(iv) Encryption and Decryption. Implement a mechanism to encrypt and decrypt electronic protected health information. Requirements addressed include: Encryption and Integrity.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
  - 164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. Requirements addressed include: Auditing.
  - 164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
  - 164.312(d) Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. Requirements addressed include: Access Control and Auditing.

Sample Configuration

Cisco ASA firewalls are designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership.

Cisco ASA firewalls are configured to use a AAA model for user-based access. Users can be assigned to groups and based on privilege levels, have access to only the information they require for their job function. By default in Cisco ASA firewalls, no users are allowed access unless specifically configured and assigned appropriate passwords. The following configuration statements create an authentication group called *Oncology*, which is assigned to various interfaces. This group uses the TACACS+ protocol to communicate with the Cisco ACS server where individual user groups and roles are configured, limiting and logging access as appropriate.

```
aaa-server CiscoACS protocol tacacs+
aaa-server CiscoACS (inside) host 192.168.42.131
 key *****
user-identity default-domain LOCAL

aaa accounting ssh console CiscoACS
aaa accounting enable console CiscoACS
aaa accounting command privilege 15 CiscoACS
aaa authentication secure-http-client
aaa local authentication attempts max-fail 6
aaa authorization exec authentication-server
```

Local individual user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration as specified in established policies for passwords.

```
username csmadmin password <removed> encrypted privilege 15
username janoff password <removed> encrypted privilege 15
username bart password <removed> encrypted privilege 15
```

It is a best practice that these local accounts represent only a subset of key network or security device administrators that would need administrative access in the event central authentications services are unavailable. This should not be the complete list of users that require access to ePHI.

These AAA authentication groups are assigned to the administrative interfaces where users connect.

```
aaa authentication ssh console CiscoACS LOCAL
aaa authentication enable console CiscoACS LOCAL
aaa authentication http console CiscoACS LOCAL
```

Cisco ASA firewalls are configurable to restrict traffic through the use of object and service-based access lists, thereby addressing Safeguard 164.308(a)(4)(ii)(A), which requires isolating healthcare information. By default, the firewall does not forward any traffic unless explicitly permitted.

The following configuration example shows how objects identify hosts and services within the network and their use in an access list to permit approved traffic:

```
!
interface outside
nameif north
bridge-group 1
security-level 0
!
interface inside
nameif south
bridge-group 1
security-level 100
!
! ----Defining Objects and Object Groups----
!
object-group network EMC-NCM
description EMC Network Configuration Manager
network-object 192.168.42.122 255.255.255.255
object-group network CSManager
description Cisco Security Manager
network-object 192.168.42.133 255.255.255.255
object-group network RSA-enVision
description RSA EnVision Syslog collector and SIM
network-object 192.168.42.124 255.255.255.255
object-group network AdminStation3
network-object 192.168.42.138 255.255.255.255
object-group network Admin-Systems
group-object EMC-NCM
group-object AdminStation
group-object AdminStation2
group-object CSManager
group-object RSA-enVision
group-object AdminStation3
group-object AdminStation4-bart
!
object-group service CSM_INLINE_svc_rule_77309411635
description Generated by CS-Manager from service of FirewallRule# 3
(ASA-DC-1-vdc1_v1/mandatory)
service-object tcp destination eq ssh
service-object tcp destination eq https
group-object HTTPS-8443
!
object-group network CSM_INLINE_dst_rule_77309411635
description Generated by CS-Manager from dst of FirewallRule# 3
(ASA-DC-1-vdc1_v1/mandatory)
group-object DC-ALL
group-object Stores-ALL
group-object DC-DMZ
!
```

```
! ----One line of the larger access-list permitting traffic----
!
access-list CSM_FW_ACL_south extended permit object-group
CSM_INLINE_svc_rule_77309411635 object-group Admin-Systems object-group
CSM_INLINE_dst_rule_77309411635
!
! ----Applying the access-list to an interface----
!
access-group CSM_FW_ACL_south in interface south
```

Administration access to the firewall is further restricted through the use of network permit statements applied to the web and terminal interfaces. Isolating administrative access to this device enforces the perimeter of the ePHI scope of the infrastructure.

The following configuration shows the authorized management hosts for SSH and HTTPS administration, and none for Telnet.

```
http server enable
http 192.168.41.101 255.255.255.255 south
http 192.168.41.102 255.255.255.255 south
http 192.168.42.122 255.255.255.255 south
http 192.168.42.124 255.255.255.255 south
http 192.168.42.133 255.255.255.255 south
http 192.168.42.138 255.255.255.255 south
telnet timeout 5
ssh 192.168.41.101 255.255.255.255 south
ssh 192.168.41.102 255.255.255.255 south
ssh 192.168.42.122 255.255.255.255 south
ssh 192.168.42.124 255.255.255.255 south
ssh 192.168.42.133 255.255.255.255 south
ssh 192.168.42.138 255.255.255.255 south
```

It is a recommended practice to enable only management interface protocols that use strong encryption, to best protect the ePHI information and the identities and passwords of those who must have access. Cisco ASA firewalls support strong encryption for SSH and HTTPS. The following configurations are used to configure strong cryptography:

```
! ---Specify only Strong algorithms for SSL connections---
ssl encryption 3des-sha1 aes128-sha1 aes256-sha1
!
! ---Specify strong encryption version of SSH---
ssh version 2
!
```

SNMP versions 1 and 2(c) transmit data between the SNMP server and the SNMP agent in the clear. This makes your infrastructure and corresponding infrastructure devices vulnerable to attack and/or misuse. SNMP v3 adds authentication and privacy options to secure its communication between SNMP servers and SNMP agents.

Cisco ASA firewalls allow secure administration using SNMP version 3 with encryption and authentication using the priv security model.

SNMP groups provide an access control policy to which users are added. The user inherits the security model of the group.

SNMP users are assigned a username, a group to which they belong, authentication password, encryption password, and associated algorithms to use. Authentication algorithms are MD5 and SHA. Encryption algorithms are DES, 3DES, and AES (128,192,256).

```
snmp-server enable
snmp-server group V3Group v3 priv
snmp-server user ciscolms V3Group v3 auth sha <AUTHENTICATION-PASSWORD> priv aes 256
<ENCRYPTION-KEY>
```

```
snmp-server user csmadmin V3Group v3 auth sha <AUTHENTICATION-PASSWORD> priv aes 256
<ENCRYPTION-KEY>
```

VPNs enable secure communication between locations by encrypting and decrypting traffic addressing Safeguard 164.312(a)(ii)(iv).

The following configurations show the setup of the additional AAA RADIUS server and authentication group for SSL VPN access from external sources.

```
aaa-server partnerauth protocol radius
aaa-server partnerauth (inside) host 192.168.42.137
timeout 5
key *****
radius-common-pw *****
webvpn
enable outside
internal-password enable
smart-tunnel list AllExternalApplications All-Applications * platform windows
group-policy DfltGrpPolicy attributes
webvpn
url-list value page1
smart-tunnel enable AllExternalApplications
group-policy HEALTH-HIPAA internal
group-policy HEALTH-HIPAA attributes
vpn-tunnel-protocol ssl-clientless
!
tunnel-group DefaultRAGroup general-attributes
authentication-server-group partnerauth
tunnel-group DefaultWEBVPNGroup general-attributes
authentication-server-group partnerauth
tunnel-group ComplianceLab type remote-access
tunnel-group ComplianceLab general-attributes
authentication-server-group partnerauth LOCAL
default-group-policy HEALTH-HIPAA
```

Cisco ASA firewalls track individual administrator actions, which address all of the HIPAA Auditing safeguards summarized above, through several mechanisms including AAA, logging, and system events by implementing the following configuration statements:

```
logging enable
logging timestamp
logging trap informational
logging asdm informational
logging host south 192.168.42.124
```

An SNMP host is the server to which SNMP notifications and traps are sent. SNMP v3 hosts require the SNMP server IP address and SNMP username. Each SNMP host can have only one username associated with it. The user credentials on the NMS (CiscoPrime, EMC NCM, and so on) must match the SNMP username credentials.

```
snmp-server host south 192.168.42.134 version 3 ciscolms
snmp-server host south 192.168.42.139 version 3 ciscolms
snmp-server host south 192.168.42.133 version 3 csmadmin
```

Enable the SNMP traps (this will change depending on environment and business requirements). The following example enables all, but this could be limited to a subset of traps.

```
snmp-server enable traps all
snmp-server location Building SJC-17-1 Aisle 1 Rack 3
snmp-server contact EmployeeA
```

In addition to being able to set timeout limits for remote access VPNs, Safeguard 164.312(a)(2)(ii) Automatic Logoff, requires that the administrative sessions to the Cisco ASA firewalls be limited with the following configurations:

```
http server idle-timeout 15
ssh timeout 15
console timeout 15
```

As a best practice, NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. Cisco ASA firewalls use NTP by implementing the following configuration statements:

```
ntp server 192.168.62.162 source south
ntp server 192.168.62.161 source south prefer
clock timezone PST -8
clock summer-time PDT recurring
```

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002 and NIST Security Publications.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Cisco Virtual Security Gateway

The Cisco Virtual Security Gateway (VSG) for Cisco Nexus 1000V Series Switches was used in the data center for setting a boundary between the sensitive scope of the organization's ePHI data environment and out-of-scope networks. It is a virtual firewall for Cisco Nexus 1000V Series Switches that delivers security and compliance for virtual computing environments. Cisco VSG uses virtual service data path (vPath) technology embedded in the Cisco Nexus 1000V Series Virtual Ethernet Module (VEM), offering transparent firewall insertion and efficient deployment. All the policy management for VSG is done via Virtual Network Management Center (VNMC). Cisco VSG provides the following:

- Zone-based security controls based on network as well as virtual machine attributes. This flexibility simplifies security policies, which are easy to troubleshoot and audit.
- Secure multi-tenant deployment, protecting tenant workloads on a shared compute infrastructure.
- Leverages vPath intelligence for efficient network-wide deployment and accelerated performance through fast-path off-load.
- IT security, network, and server teams to collaborate while enabling administrative segregation to meet regulatory and audit requirements and reduce administrative errors.

Table 5-29 PHI HIPAA Assessment Summary—Cisco Virtual Security Gateway

Models Assessed	
Nexus VSG version 4.2(1)VSG1(1)	
HIPAA Safeguards Addressed	
Administrative	**Standards/Implementation Specifications**

Table 5-29 PHI HIPAA Assessment Summary—Cisco Virtual Security Gateway (continued)

164.308	(a)(1)(i) Security Management Process
	(a)(1)(ii)(D) Information System Activity Review
	(a)(3)(i) Authorization/Supervision
	(a)(4)(ii)(A) Isolating health care clearinghouse function
	(a)(4)(i) Access Authorization
	(a)(4)(ii)(C) Access Est./Modification
	(a)(5)(i) Log-in Monitoring
	(a)(6)(i) Security Incident Procedures
	(a)(6)(i) Response and Reporting
Technical	**Standards/Implementation Specifications**
164.312	(a)(i) Access Control
	(a)(2)(i) Unique User Identification
	(a)(2)(ii) Emergency Access procedures
	(a)(2)(ii) Automatic Logoff
	(a)(ii)(iv) Encryption and Decryption
	(b) Audit Controls
	(c)(1) Data Integrity
	(d) Person or Entity Authentication
	(e)(i) Transmission Security
	(e)(2)(i) Integrity Controls
	(e)(2)(ii) Encryption
HIPAA Standards Failed	
No HIPAA standards were failed.	
HIPAA Implementation Specifications Failed	
No HIPAA implementation specifications were failed.	

Primary PHI Function

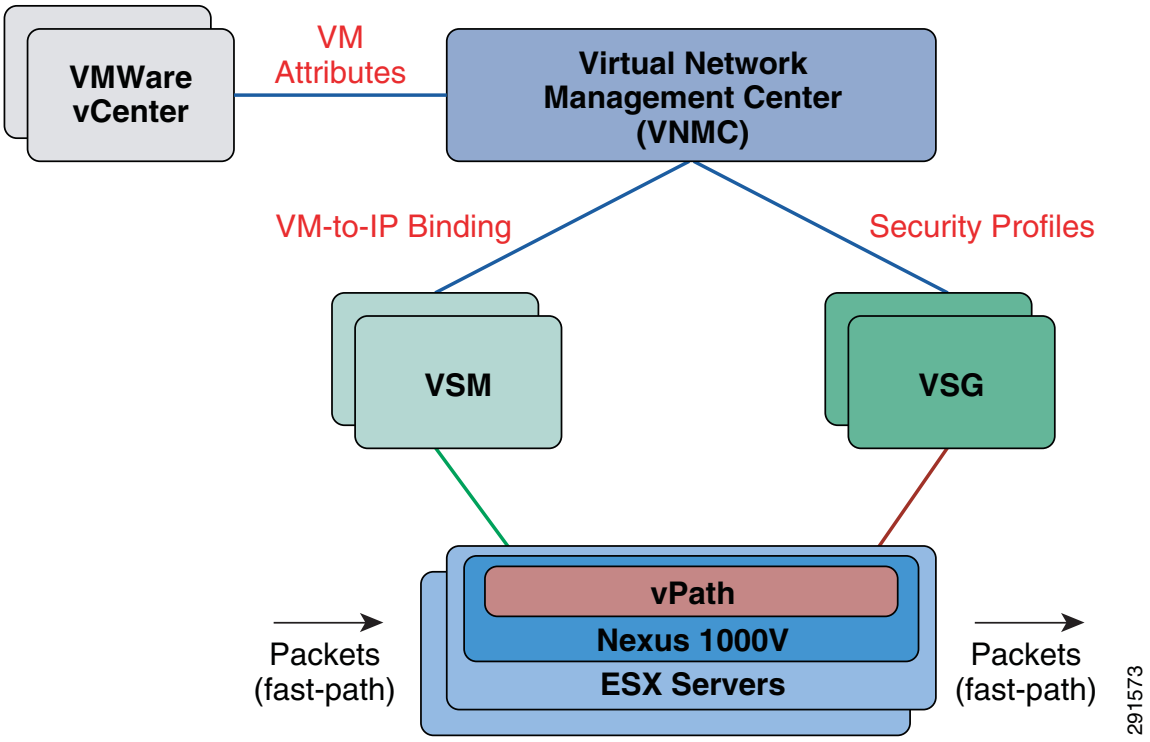
The primary function of the Cisco VSG is segmentation of PHI scope and enforcement of that new scope boundary. The Cisco VSG serves as a stateful firewall, restricting traffic between the cardholder data environment and other areas of the network.

Design Considerations

Cisco VSG integrates with Cisco Nexus 1000V Series Switches to enforce security policies for your virtualized environment. VNMC provides policy management for a multitenant environment. One or more VSGs are required per tenant. VSG uses the vPath intelligence in the Virtual Ethernet Module (VEM) of the Cisco Nexus 1000V Series to provide the security policy enforcement.

Cisco VSG is deployed as a virtual appliance in vCenter. The primary function of Cisco VSG is to protect against unauthorized access to the cardholder environment. (See Figure 5-114.)

Figure 5-114 Cisco Nexus VSG System Architecture



HIPAA Assessment Detail—HIPAA Safeguards Addressed

HIPAA safeguards are spread across multiple categories. The VSG firewall helps healthcare covered entities and business associates meet access control safeguards in the Administrative and Technical categories. The access control can be applied to both internal and external users that access ePHI data. Additionally, controls to protect the administrator accounts on the firewall have been implemented to protect the firewall from unauthorized modification if the authentication server fails. These local accounts represent only a subset of select individuals that would need access in the event central authentications services are unavailable.

All of the sample configurations of the VSG shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.308(a)(4)(ii)(A) Isolating healthcare clearinghouse function. If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.

  - §164.308(a)(4)(ii)(C) Access Establishment and Modification. Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. Requirements addressed include: Access Control, Incident Response and Auditing.
  - §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).
  - §164.312(d) Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. Requirements addressed include: Access Control and Auditing.
  - §164.308(a)(5)(ii)(D) Password Management. Procedures for creating, changing, and safeguarding passwords. Requirements addressed include: Access Control and Auditing.
- Integrity—Protect electronic protected health information from improper alteration or destruction as required by HIPAA Technical safeguards.
  - §164.312(c)(1) Data Integrity. Implement policies and procedures to protect health information from improper alteration or destruction.
  - §164.308(a)(4)(ii)(C) Access Establishment and Modification. Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. Requirements addressed include: Access Control, Incident Response, and Auditing.
  - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
  - §164.312(a)(2)(ii) Emergency Access Procedure. Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.
  - §164.312(e)(1) Transmission Security. Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network. Requirements addressed include: Encryption and Integrity.
  - §164.308(e)(2)(i) Integrity Controls. Implement security measures to ensure that ePHI is not improperly modified without detection until disposed of. Requirements addressed include: Integrity.
  - §164.308(e)(2)(ii) Encryption. Implement a mechanism to encrypt ePHI whenever deemed appropriate. Requirements addressed include: Encryption.
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
  - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
  - §164.312(a)(2)(i) Unique User Identification. Assign a unique name and/or number for identifying and tracking user identity. Requirements addressed include: Access Control and Auditing.
  - §164.312(a)(2)(ii) Automatic logoff. Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. Requirements addressed include: Access Control and Auditing.

- Encryption—Implement mechanisms to encrypt and decrypt ePHI.
  - §164.312(a)(ii)(iv) Encryption and Decryption. Implement a mechanism to encrypt and decrypt electronic protected health information. Requirements addressed include: Encryption and Integrity.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
  - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. Requirements addressed include: Auditing.
  - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
  - §164.312(d) Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. Requirements addressed include: Access Control and Auditing.

Sample Configuration

Cisco VSG firewalls are designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership.

User roles in VNMC contain one or more privileges that define the operations allowed for the user who is assigned the role. A user can be assigned one or more roles. A user assigned multiple roles has the combined privileges of all assigned roles. For example, if Role1 has policy-related privileges, and Role2 has tenant-related privileges, users who are assigned to both Role1 and Role2 have policy and tenant related privileges.

The system contains the following default user roles:

- aaa—User has read and write access to users, roles, and AAA configuration. Read access to the rest of the system.
- admin—User has complete read-and-write access to the entire system and has all privileges. The default admin account is assigned this role by default, and it cannot be changed.
- network—User creates organizations, security policies, and device profiles.
- operations—User acknowledges faults and performs some basic operations such as logging configuration.
- read-only—User has read-only access to system configuration and operational status with no privileges to perform any operations.

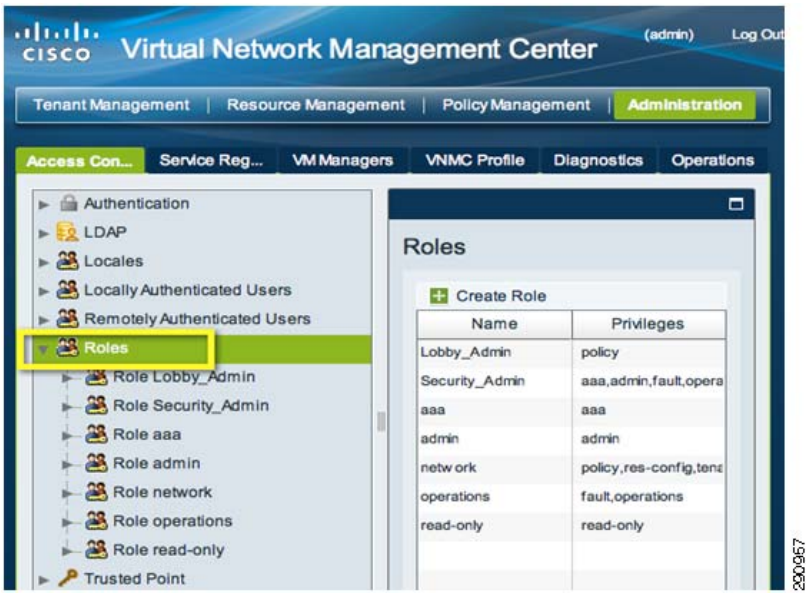
Roles can be created, modified to add new or remove existing privileges, or deleted. When a role is modified, the new privileges are applied to all users assigned to that role. Privilege assignment is not restricted to the privileges defined for the default roles. That is, you can use a custom set of privileges to create a unique role. For example, the default Network and Operations roles have different sets of privileges, but a new Network and Operations role can be created that combines the privileges of both roles.

To configure roles in VNMC, do the following:

1. Click the **Administration** tab, then click the **Access Control** sub-tab.

2. In the Navigation pane, select the **Roles** node. In the Work pane, click **Create Roles** (see Figure 5-115.)

Figure 5-115 Configuring Roles



In addition to roles, the user is also provided another dimension of privilege, which limits the user to tenant level visibility, called *locale*. Each locale defines one or more organizations (domains) to which the user is allowed access, and access would be limited to the organizations specified in the locale. To configure locales in VNMC, do the following:

1. Click the Administration tab, then click the Access Control sub-tab.
2. In the Navigation pane, select the Locales node.
3. In the Work pane, click the Create Locale link. (See Figure 5-116.)

Figure 5-116 Configuring Locales

CLI configuration of AAA services is as follows:

```
tacacs-server key 7 "<removed>"
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
    use-vrf management
    source-interface mgmt0
aaa group server tacacs+ tacacs
!
aaa authentication login default group CiscoACS
aaa authentication login console group CiscoACS

HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of automatic logoff options.
Cisco VSG supports session timeout. It is a best practice to set session time-out to
15 minutes,
line vty
  exec-timeout 15
line console
  exec-timeout 15
```

It is a recommended practice to only enable management interface protocols which use strong encryption in order to best protect the ePHI information and the identities and passwords of those who must have access. Cisco VSG firewalls support strong encryption for SSH and HTTPS. Only SSH access is allowed for firewall console access over the network. The communication between Cisco VSG and Management Platform (VNMC) is all encrypted over SSL (443)

Cisco Nexus VSG can be configured to use secure protocols for all system functions. This includes SSH for remote management, SCP, and SFTP for file transfers. Insecure services can be disable or blocked using configuration statements and access lists.

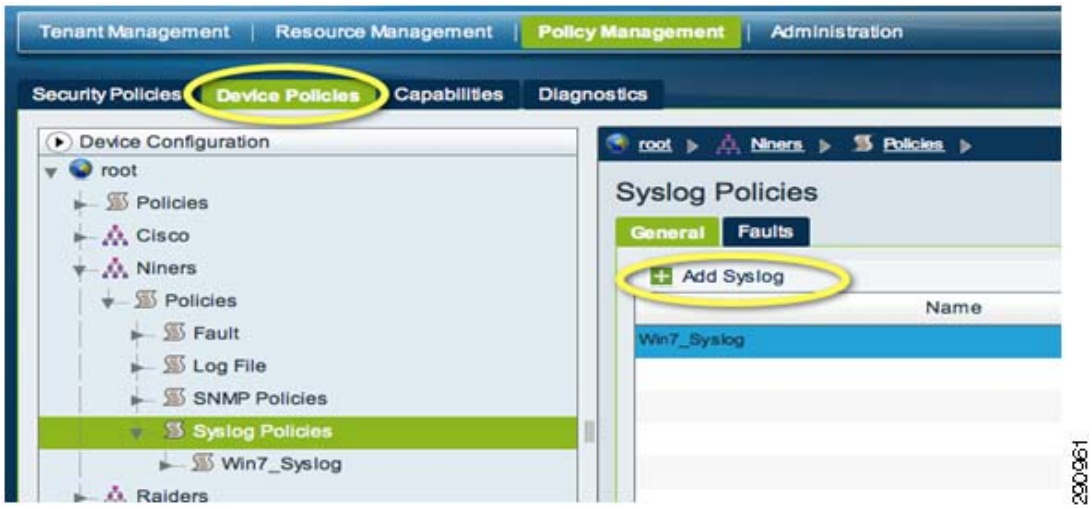
```
no feature telnet
no telnet server enable
feature ssh
```

Cisco Nexus VSG support administrative protocols with strong cryptography such as SSH version 2.

Cisco ASA firewalls track individual administrator actions, which address all of the HIPAA Auditing Safeguards summarized above, through several mechanisms including AAA, logging, and system events by implementing the following syslog server configurations for Cisco VSG to send all the logging information to a standard syslog server. This setting is available as part of the device profile.

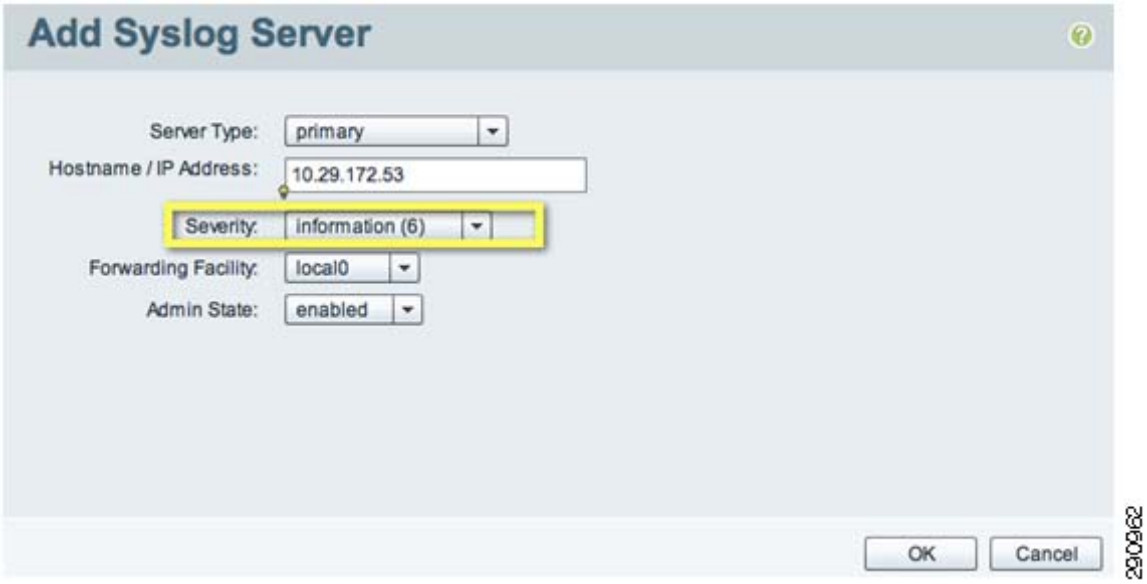
1. Navigate to Policy Management > Device Policies > Tenant> Policies > Syslog Policies. Add a syslog policy, as shown in Figure 5-117.

Figure 5-117 Configuring Syslog



2. The severity of the logging should be at level 6 to capture the firewall policy hit in the VSG. (See Figure 5-118).

Figure 5-118 Configuring Logging Severity



3. The syslog policy is attached to the Device Profile to enable the settings in the VSG.

   CLI configuration of logging services is as follows:

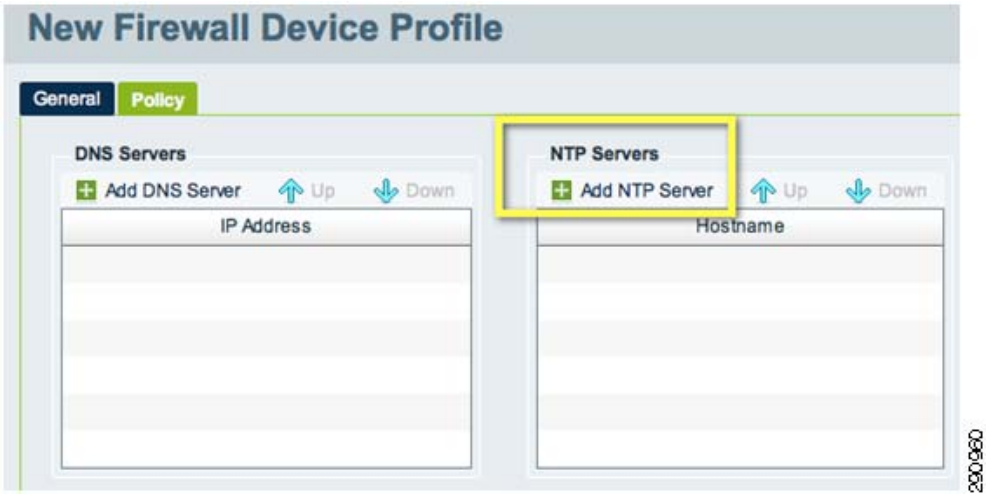
```
logging logfile messages 2
logging server 192.168.42.124 6 facility local0
logging monitor 2
```

As a best practice, NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

NTP is configured in the Firewall Device Profile for the Cisco VSG VNMC. The setting is published via the device policy to Cisco VSG.

1. In the navigation pane, click the Policy Management tab, then the Device Policies sub-tab, and expand the Device Profile for a tenant.
2. Click a Profiles node to add a firewall device profile, and you see the option to add NTP server, as shown in Figure 5-119.

Figure 5-119 Configuring NTP



HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Intrusion Detection

Cisco Catalyst 6500 Series Intrusion Detection System Services Module 2

The Cisco Catalyst 6500 Series Intrusion Detection System Services Module 2 (IDSM2) is an important intrusion prevention system (IPS) solution that protects switched environments by integrating full-featured IPS functions directly into the network infrastructure through the widely deployed Cisco Catalyst chassis. This integration allows the user to monitor traffic directly off the switch backplane.

The Cisco IDSM2 with Cisco IPS Sensor Software v6.0 helps users stop more threats through the use of the following elements:

- Multivector threat identification—Detailed inspection of Layer 2–7 traffic protects your network from policy violations, vulnerability exploitations, and anomalous activity.
- Accurate prevention technologies—The innovative Cisco Risk Rating feature and Meta Event Generator provide the ability to take preventive actions on a broader range of threats without the risk of dropping legitimate traffic.

When combined, these elements provide a comprehensive inline prevention solution, providing the ability to detect and stop the broadest range of malicious traffic before it affects business continuity.

Table 5-30 PHI HIPAA Assessment Summary—Cisco IDSM2

Models Assessed	
WS-SVC-IDSM-2 version 7.0(4)	
HIPAA Safeguards Addressed	
Administrative	**Standards/Implementation Specifications**
164.308	(a)(1)(i) Security Management Process
	(a)(3)(i) Authorization/Supervision
	(a)(4)(i) Access Authorization
	(a)(5)(ii)(B) Protection from Malicious Software
	(a)(5)(ii)(C) Log-in Monitoring
	(a)(6)(i) Security Incident Procedures
	(a)(6)(i) Response and Reporting
Technical	**Standards/Implementation Specifications**
164.312	(a)(i) Access Control
	(b) Audit Controls
HIPAA Standards Failed	
No HIPAA standards were failed.	
HIPAA Implementation Specifications Failed	
No HIPAA implementation specifications were failed.	

Primary PHI Function

The primary function of the Cisco IDSM2 is to monitor all traffic at the perimeter of the ePHI data environment as well as at critical points inside of the ePHI data environment, and alert personnel to suspected compromises.

Design Considerations

- Configure the Cisco IDSM2 to lock accounts so that users cannot keep trying to login after a certain number of failed attempts.
- Allow secure management of the Cisco IDSM2 only from specific host/hosts.
- Configure appropriate banner messages on login. The login banner warning should not reveal the identity of the company that owns or manages the Cisco IDSM2. The banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Change default passwords and community strings to appropriate complexity.

For more information, see the Installation Guide at the following URL:

http://www.cisco.com/en/US/docs/security/ips/6.0/configuration/guide/cli/cliInter.html

HIPAA Assessment Detail—HIPAA Safeguards Passed

All of the sample configurations of the IDSM shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
  - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
  - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
  - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
  - §164.308(a)(5)(ii)(B) Protection from malicious software. Procedures for guarding against, detecting, and reporting malicious software. Requirements addressed include: Incident Response and Auditing.
  - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
  - §164.308(a)(6)(i) Security Incident Procedures. Implement policies and procedures to address security incidents. Requirements addressed include: Incident Response and Auditing.

  - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.

- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
  - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. Requirements addressed include: Auditing.
  - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.

Sample Configuration

Cisco IDSM modules are designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership.

Cisco IDSM2 modules are configured to use a AAA model for user-based access. Users can be assigned to groups and based on privilege levels and have access to only the information they require for their job function. By default, no users are allowed access unless specifically configured and assigned appropriate passwords. The following configuration statements use the RADIUS protocol to communicate with the Cisco ACS server where individual user groups and roles are configured, limiting and logging access as appropriate.

```
! ------------------------------
service aaa
aaa radius
primary-server
server-address 192.168.42.131
shared-secret <removed>
exit
nas-id DMZ-IDS1
local-fallback enabled
console-authentication radius-and-local
default-user-role administrator
exit
exit
! ------------------------------
```

Cisco IDSM2 modules allow only administrative connections from authorized hosts/networks as specified in the device configuration. The following configuration shows the authorized management hosts for SSH and HTTPS administration, and disabling of Telnet.

```
! ------------------------------
service host
network-settings
host-ip 192.168.21.94/24,192.168.21.1
host-name DMZ-IDS2
telnet-option disabled
access-list 192.168.41.101/32
access-list 192.168.41.102/32
access-list 192.168.42.122/32
access-list 192.168.42.124/32
access-list 192.168.42.133/32
access-list 192.168.42.138/32
```

Local individual user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration as specified in established policies for passwords.

Cisco IDSM2 modules support the ability to specify a minimum password length for local accounts.

```
! ------------------------------
service authentication
password-strength
size 7-64
! ------------------------------
```

Cisco IDSM2 modules support the ability to specify alphanumeric passwords for local accounts.

```
! ------------------------------
service authentication
password-strength
digits-min 1
lowercase-min 1
other-min 1
! ------------------------------
```

Cisco IDSM2 modules support the ability to specify that old passwords should not be re-used for local accounts.

```
! ------------------------------
service authentication
password-strength
number-old-passwords 4
! ------------------------------
```

Cisco IDSM2 modules support the ability to specify that only a limited number of attempts can be made when authenticating for local accounts.

```
! ------------------------------
service authentication
attemptLimit 6
! ------------------------------
```

Cisco IDSM2 modules support the ability to lockout local accounts after the specified number of failed attempts, requiring an administrator to re-enable them. Locked accounts are indicated by parentheses when using the show users command:

```
sensor# show users all
CLI ID  User       Privilege
* 1349  bart       administrator
  5824 (pauljones) viewer
  9802  christian  operator
```

Cisco IDSM2 modules are capable of performing intrusion detection and prevention through the use of VLAN interfaces from the host Cisco Catalyst service chassis addressing safeguard 164.308(a)(1)(i) Security Management. IPS signature updates and configurations are managed centrally through Cisco Security Manager. The following configuration statements are necessary in the Cisco Catalyst service chassis to forward traffic via VLANs and enable the IDS inspection capability:

```
!
!
intrusion-detection module 2 management-port access-vlan 21
intrusion-detection module 2 data-port 1 trunk allowed-vlan 83,84
!
```

Cisco IDSM2 module interfaces are configured as follows to receive, inspect, and forward traffic across the assigned VLANs:

```
! -----------------------------
service interface
physical-interfaces GigabitEthernet0/7
subinterface-type inline-vlan-pair
subinterface 1
description INT1 vlans 83 and 84
vlan1 83
vlan2 84
exit
exit
exit
exit
! -----------------------------
```

To address the Incident Response and Auditing HIPAA Safeguards identified above, Cisco IDSM can be configured to send its log data to the RSA enVision log management platform. RSA enVision collects information from all devices to ensure the integrity and correlation of events.

Cisco IDSM2 modules are capable of sending system events to a centralized repository using SNMP traps. Logs stored locally are buffered and require operator level privileges on the device to be viewed. External logging is enabled by implementing the following configuration statements to send them to the RSA enVision server:

```
! -----------------------------
service notification
trap-destinations 192.168.42.124
trap-community-name RSAenVision
exit
enable-notifications true
trap-community-name RSAenVision
exit
! -----------------------------
```

As a best practice, NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP server was hosted at the data center site. Cisco IDSM2 uses NTP to meet these requirements by implementing the following configuration statements:

```
time-zone-settings
offset -8
standard-time-zone-name PST
exit
ntp-option enabled-ntp-unauthenticated
ntp-server 192.168.62.161
exit
summertime-option recurring
summertime-zone-name PDT
```

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

CHAPTER 6

Summary

HIPAA is flexible and open to interpretation based on the type of healthcare entity. Cisco customers have asked for clarification in relation to the common architectures and security products that might be utilized. In response, Cisco contracted Verizon Business to assess Cisco's enterprise reference architectures and components. Verizon provides design guidance and explains the rationale that they used for assessing healthcare entities in the context of Cisco's enterprise solution set.

This Cisco Compliance Solution for HIPAA Security Rule provides a reference architecture designed to help covered entities and business associates clarify compliance with the HIPAA Security Rule by mapping architectures and products to the HIPAA Security Rule Technical Safeguards, standards, and implementation specifications.

Compliance is a journey, not a destination. It requires continual attention to maintain. It is a journey that cannot be traveled alone. Trusted advisors such as auditors and vendors simplify the goal of maintaining compliance. The following provides a summary of the assessment results.

HIPAA Solution Summary Results

Table 6-1 lists the HIPAA citations that were addressed within the solution.

Table 6-1 HIPAA Citations Addressed

Citation	Title
164.308(a)(1)(i)	Security Management Process
164.308(a)(1)(ii)(D)	Information System Activity Review
164.308(a)(3)(ii)(A)	Authorization and/or Supervision
164.308(a)(3)(ii)(C)	Termination Procedures
164.308(a)(4)(ii)(A)	Isolating Health Care Clearinghouse Function
164.308(a)(4)(ii)(B)	Access Authorization
164.308(a)(4)(ii)(C)	Access Establishment and Modification
164.308(a)(5)(ii)(B)	Protection from Malicious Software
164.308(a)(5)(ii)(C)	Log-in Monitoring

Table 6-1 HIPAA Citations Addressed (continued)

164.308(a)(5)(ii)(D)	Password Management
164.308(a)(6)(ii)	Response and Reporting
164.308(a)(7)(i)	Contingency Plan
164.308(a)(8)	Evaluation
164.310(a)(2)(iii)	Facility Access Control and Validation Procedures
164.312(a)(2)(i)	Unique User Identification
164.312(a)(2)(ii)	Emergency Access Procedure
164.312(a)(2)(iii)	Automatic Logoff
164.312(a)(2)(iv)	Encryption and Decryption
164.312(b)	Audit Controls
164.312(c)(1)	Data Integrity
164.312(d)	Person or Entity Authentication
164.312(e)(2)(i)	Transmission Integrity Controls
164.312(e)(2)(ii)	Transmission Encryption

Lessons Learned

Addressing the individual HIPAA safeguards without an encompassing security framework is difficult; there are many grey areas that are contested by auditors and interpretations that can be made for corner cases. The best strategy is to use a common control structure that addresses multiple compliance standards using a “unified compliance” mindset. The intent is that regardless of the type of sensitive data, a single security strategy should meet the needs of an organization to protect it from a compliance perspective.

As an example, there is no specific mention of firewall technology in the HIPAA standard because HIPAA is written to be flexible enough to address all types of healthcare entities. However, when considering the common risks that are associated with enterprise organizations, such as the Internet and partner connections that share ePHI, Verizon cites the following controls that inductively requires the use of a firewall:

- 164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
- 164.308(a)(4)(ii)(A) Isolating healthcare clearinghouse function. If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.

The word *procedures* requires the use of a technology to address the commensurate risk. In organizations that are represented in the Cisco solution, the Internet is a tremendous threat that can be addressed only through the use of a stateful firewall.

In HIPAA, regardless of inconsistencies and specifics from interpretation, the resonant idea is that reasonable controls must be in place to mitigate existing risks that threaten the integrity and ownership of sensitive Healthcare data. By implementing a broader and often more specific common industry

security framework such as HiTrust's Common Security Framework (CSF), ISO 27002, or NIST Security Publications, as well as other industry-based standards, a comprehensive policy can be tailored to address the risk and governance needs specific to the enterprise organization.

APPENDIX A

Bill Of Material

Each Cisco Validated Design is a point-in-time effort. The following bill of materials represents the products selected before testing. Large encompassing validation efforts can take a significant length (12–18 months) to complete, during which product models may become outdated. Enterprise compliance needs can often still be met using newer/current versions of similar product lines and models.

The HIPAA assessment/validation of the existing laboratory infrastructure that was previously used for PCI compliance did not include any product updates, and therefore this bill of materials may contain items and models that are no longer available for sale.

Managed Service Provider Clinic

Name	Catalog Num	Vendor	Description	Qty
AIR-CAP3502I-A-K9	AIR-CAP3502I-A-K9	Cisco	802.11a/g/n Ctrlr-based AP w/CleanAir; Int Ant; A Reg Domain	5
AIR-AP-BRACKET-1	AIR-AP-BRACKET-1	Cisco	Cisco 1040/1140/1260/3500 Low Profile Mounting Bracket (Default)	5
AIR-AP-T-RAIL-R	AIR-AP-T-RAIL-R	Cisco	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	5
CON-SNT-CAP352IA	CON-SNT-CAP352IA	Cisco	Cisco SMARTNET 8X5XNBD 802.11a/g/n Ctrlr-based AP w/CleanAir; I	5
S3G1RK9W8-12423JA	S3G1RK9W8-12423JA	Cisco	Cisco 3500 Series IOS Wireless LAN Controller-based Recovery	5
AIR-WLC2125-K9	AIR-WLC2125-K9	Cisco	Cisco 2100 Series WLAN Controller for up to 25 Lightweight APs	1
ASA5505-PWR-AC	ASA5505-PWR-AC	Cisco	Cisco ASA 5505 AC Power Supply Adapter	1
SSC-BLANK	SSC-BLANK	Cisco	Cisco ASA 5505 SSC Blank Slot Cover	1

SWLC2100K9-70-ER	SWLC2100K9-70-ER	Cisco	Cisco Unified Wireless Controller SW Release 7.0	1
CAB-AC-C5	CAB-AC-C5	Cisco	AC Power Cord, Type C5, US	1
CON-SNT-AC2125K9	CON-SNT-AC2125K9	Cisco	SMARTNET 8X5XNBD WLAN Controller	1
SWLC2100K9-70	SWLC2100K9-70	Cisco	Cisco Unified Wireless Controller SW Release 7.0	1
ASA5515-IPS-K9	ASA5515-IPS-K9	Cisco	ASA 5515-X with IPS, SW, 6GE Data, 1GE Mgmt, AC, 3DES/AES	1
ASA5500-SC-5	ASA5500-SC-5	Cisco	ASA 5500 5 Security Contexts License	1
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	1
SF-ASA-9.1-K8	SF-ASA-9.1-K8	Cisco	ASA 5500 Series Software Ver. 9.1 for ASA 5512X--5555X, DES	1
SF-ASAIPS64-7.1-K9	SF-ASAIPS64-7.1-K9	Cisco	ASA 5500-X IPS Software 7.1 for IPS SSP	1
ASA5515-IPS-SSP	ASA5515-IPS-SSP	Cisco	ASA 5515-X IPS SSP License	1
ASA5500-ENCR-K9	ASA5500-ENCR-K9	Cisco	ASA 5500 Strong Encryption License (3DES/AES)	1
CON-OSP-ASAUC24	CON-OSP-ASAUC24	Cisco	ONSITE 24X7X4 ASA-UC-24	1
CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	4
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	4
CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	4
CIVS-IPC-2421	CIVS-IPC-2421	Cisco	Cisco Indoor SD IP Dome, 2.8-10mm, D/N, Smoked, CM	1
CON-SNT-IPC2421	CON-SNT-IPC2421	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2421	1
CIVS-IPC-2500	CIVS-IPC-2500	Cisco	Cisco 2500 IP Camera, Full Resolution, Day/Night	1
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	1
CIVS-IPC-VT55	CIVS-IPC-VT55	Cisco	Cisco IP Camera Tamron 5-50mm Varifocal Lens	1
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	1
CON-SNT-IPC2500	CON-SNT-IPC2500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2500	1
CIVS-IPC-2520V	CIVS-IPC-2520V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, VR	1

CON-SNT-IPC2520	CON-SNT-IPC2520	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2520V	1
CIVS-IPC-2521V	CIVS-IPC-2521V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, Smoked, VR	1
CON-SNT-IPC2521	CON-SNT-IPC2521	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2521V	1
CIVS-IPC-4500	CIVS-IPC-4500	Cisco	Cisco 4500 IP Camera, HD, DSP, Day/Night	1
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	1
CIVS-IPC-VFM15-50	CIVS-IPC-VFM15-50	Cisco	Cisco IP Camera Lens Megapixel 15-50mm Fujinon	1
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	1
CON-SNT-IPC4500	CON-SNT-IPC4500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-4500	1
CIVS-IPC-5010	CIVS-IPC-5010	Cisco	Cisco Video Surveillance IP Camera, Indoor HD Dome (Clear)	1
CON-SNT-CIVSIPC1	CON-SNT-CIVSIPC1	Cisco	SMARTNET 8X5XNBD Cisco Video Surveillance IP Camera	1
CIVS-IPC-5011	CIVS-IPC-5011	Cisco	Cisco Video Surveillance IP Camera, Indoor HD Dome (Smoked)	1
CON-SNT-CIVSIPC0	CON-SNT-CIVSIPC0	Cisco	SMARTNET 8X5XNBD Cisco Video Surveillance IP Camera, Indo	1
CIVS-MSP-1RU	CIVS-MSP-1RU	Cisco	1RU MSP Assembly	1
CIVS-CAB-16-AC	CIVS-CAB-16-AC	Cisco	CIVS C16 Power Cable North America	1
CIVS-HDD-1000	CIVS-HDD-1000	Cisco	1TB SATA Drive for CIVS-MSP	4
CIVS-MS-SW6.2	CIVS-MS-SW6.2	Cisco	CIVS-MS Media Server v6.2 Software License with Hardware	1
CIVS-VSM-SW4262	CIVS-VSM-SW4262	Cisco	CIVS-VSM Video Surveillance Manager v4.2/6.2 SW Mfg Image	1
CON-SNT-VSM1U	CON-SNT-VSM1U	Cisco	SMARTNET 8X5XNBD 1RU MSP Assembly	1
CIVS-OM-SW4.1=	CIVS-OM-SW4.1=	Cisco	CIVS-OM Operations Manager v4.1 Software Only	1
CON-SAS-OMSW41	CON-SAS-OMSW41	Cisco	SW APP SUPP CIVS-OM Operations Manager v4.1 Software	1
CIVS-VM-1DFL=	CIVS-VM-1DFL=	Cisco	Cisco VS Virtual Matrix Client License, 1 client	1
CON-SAS-VSVMCL1	CON-SAS-VSVMCL1	Cisco	SW APP SUPP CIVS-VM-1DFL	1
CIVS-VM-SW6.2=	CIVS-VM-SW6.2=	Cisco	CIVS-VM Virtual Matrix v6.2 Software License	1

CON-SAS-VMSW62	CON-SAS-VMSW62	Cisco	SW APP SUPP CIVS-VM Virtual Matrix v6.2 Software Lic	1
WS-C2960S-48FPS-L	WS-C2960S-48FPS-L	Cisco	Catalyst 2960S 48 GigE PoE 740W, 4 x SFP LAN Base	1
CAB-L620P-C13-US	CAB-L620P-C13-US	Cisco	Power Cord, 250VAC, 15A, NEMA L6-20 to C13, US	1

Doctor's Office

Name	Catalog Num	Vendor	Description	Qty
AIR-LAP1042N-A-K9	AIR-LAP1042N-A-K9	Cisco	802.11a/g/n Fixed Unified AP; Int Ant; A Reg Domain	1
AIR-AP-BRACKET-1	AIR-AP-BRACKET-1	Cisco	1040/1140/1260/3500 Low Profile Mounting Bracket (Default)	1
AIR-AP-T-RAIL-R	AIR-AP-T-RAIL-R	Cisco	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	1
CON-SNT-L1042A	CON-SNT-L1042A	Cisco	SMARTNET 8X5XNBD 802.11a/g/n Fixed Un	1
S104RK9W-12423JA	S104RK9W-12423JA	Cisco	Cisco 1040 Series IOS WIRELESS LAN LWAPP RECOVERY	1
CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	1
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	1
CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	1
CISCO891W-AGN-A-K9	CISCO891W-AGN-A-K9	Cisco	Cisco 891 GigaE SecRouter w/ 802.11n a/b/g FCC Comp	1
AIR-ANTM2050D-R	AIR-ANTM2050D-R	Cisco	2.2dBi/2.4Ghz,5.0dBi/5GHz DualBand Dipole Antenna	3
CAB-AC2	CAB-AC2	Cisco	AC Power cord North America	1
CAB-ETH-S-RJ45	CAB-ETH-S-RJ45	Cisco	Yellow Cable for Ethernet, Straight-through, RJ-45, 6 feet	1
ISR-CCP-EXP	ISR-CCP-EXP	Cisco	Cisco Config Pro Express on Router Flash	1
PWR-80W-AC	PWR-80W-AC	Cisco	Power Supply 80 Watt AC	1
S890VK9-15001M	S890VK9-15001M	Cisco	Cisco 890 Series IOS UNIVERSAL	1
SL-890-AIS	SL-890-AIS	Cisco	Cisco 890 Advanced IP Services License	1

800-IL-PM-4	800-IL-PM-4	Cisco	4 Port 802.3af capable pwr module for 890 Series Router	1
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	1
CON-SNT-C891WAK9	CON-SNT-C891WAK9	Cisco	SMARTNET 8X5XNBD Cisco 891 GigaE SecRouter	1
MEM8XX-512U768D	MEM8XX-512U768D	Cisco	DRAM Upgrade 512 MB to 768 MB	1
CIVS-IPC-2421	CIVS-IPC-2421	Cisco	Cisco Indoor SD IP Dome, 2.8-10mm, D/N, Smoked, CM	1
CON-SNT-IPC2421	CON-SNT-IPC2421	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2421	1
CIVS-IPC-2500	CIVS-IPC-2500	Cisco	Cisco 2500 IP Camera, Full Resolution, Day/Night	1
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	1
CIVS-IPC-VT55	CIVS-IPC-VT55	Cisco	Cisco IP Camera Tamron 5-50mm Varifocal Lens	1
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	1
CON-SNT-IPC2500	CON-SNT-IPC2500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2500	1
WS-C2960PD-8TT-L	WS-C2960PD-8TT-L	Cisco	Catalyst 2960 Powered Device 8 10/100 + 1 1000BT LAN Base	1
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	1
CON-SNT-C2960P8T	CON-SNT-C2960P8T	Cisco	SMARTNET 8X5XNBD Cat2960 Pwrd Device 8 10/100-1 1K BT LAN	1
PWR-A	PWR-A	Cisco	Pwr Sply In:100-240VAC Out:48VDC 380mA-2960PD-8TT-L	1

Mini Clinic

Name	Catalog Num	Vendor	Description	Qty
AIR-LAP1042N-A-K9	AIR-LAP1042N-A-K9	Cisco	802.11a/g/n Fixed Unified AP; Int Ant; A Reg Domain	1
AIR-AP-BRACKET-1	AIR-AP-BRACKET-1	Cisco	1040/1140/1260/3500 Low Profile Mounting Bracket (Default)	1
AIR-AP-T-RAIL-R	AIR-AP-T-RAIL-R	Cisco	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	1
CON-SNT-L1042A	CON-SNT-L1042A	Cisco	SMARTNET 8X5XNBD 802.11a/g/n Fixed Un	1

S104RK9W-12423JA	S104RK9W-12423JA	Cisco	Cisco 1040 Series IOS WIRELESS LAN LWAPP RECOVERY	1
CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	1
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	1
CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	1
CISCO1941W-A/K9	CISCO1941W-A/K9	Cisco	Cisco 1941 Router w/ 802.11 a/b/g/n FCC Compliant WLAN ISM	1
CAB-ADSL-RJ11	CAB-ADSL-RJ11	Cisco	Lavender Cable for xDSL, Straight-through, RJ-11, 6 feet	1
ISR-CCP-EXP	ISR-CCP-EXP	Cisco	Cisco Config Pro Express on Router Flash	1
S801RK9W-12421JA	S801RK9W-12421JA	Cisco	Cisco 801 Series IOS WIRELESS LAN LWAPP RECOVERY	1
S801W7K9-12421JA	S801W7K9-12421JA	Cisco	Cisco 801 Series IOS WIRELESS LAN	1
SL-19-IPB-K9	SL-19-IPB-K9	Cisco	IP Base License for Cisco 1900	1
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	1
CON-SNT-1941WA	CON-SNT-1941WA	Cisco	SMARTNET 8X5XNBD Cisco 1941 Router w/ 802.11 a/b/g/n FCC	1
HWIC-1ADSL	HWIC-1ADSL	Cisco	1-port ADSLoPOTS HWIC	1
HWIC-3G-HSPA-A	HWIC-3G-HSPA-A	Cisco	3G HWIC ATT HSPA/UMTS 850/1900/2100MHz; Quad-band 2G	1
MEM-1900-512U2.5GB	MEM-1900-512U2.5GB	Cisco	512MB to 2.5GB DRAM Upgrade (2GB+512MB) for Cisco 1941 ISR	1
MEM-CF-256U2GB	MEM-CF-256U2GB	Cisco	256MB to 2GB Compact Flash Upgrade for Cisco 1900,2900,3900	1
PWR-1941-POE	PWR-1941-POE	Cisco	Cisco 1941 AC Power Supply with Power Over Ethernet	1
S19UK9-15102T	S19UK9-15102T	Cisco	Cisco 1900 IOS UNIVERSAL	1
SL-19-SEC-K9	SL-19-SEC-K9	Cisco	Security License for Cisco 1900	1
CIVS-IPC-2421	CIVS-IPC-2421	Cisco	Cisco Indoor SD IP Dome, 2.8-10mm, D/N, Smoked, CM	1
CON-SNT-IPC2421	CON-SNT-IPC2421	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2421	1
CIVS-IPC-2500	CIVS-IPC-2500	Cisco	Cisco 2500 IP Camera, Full Resolution, Day/Night	1
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	1

CIVS-IPC-VT55	CIVS-IPC-VT55	Cisco	Cisco IP Camera Tamron 5-50mm Varifocal Lens	1
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	1
CON-SNT-IPC2500	CON-SNT-IPC2500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2500	1
WS-C2960G-8TC-L	WS-C2960G-8TC-L	Cisco	Cisco Catalyst 2960 7 10/100/1000 + 1 T/SFP LAN Base	2
CAB-AC-RA	CAB-AC-RA	Cisco	Power Cord,110V, Right Angle	2
CON-SNT-C2960G8C	CON-SNT-C2960G8C	Cisco	SMARTNET 8X5XNBD Catalyst 2960 7 10/1	2
GLC-SX-MM=	GLC-SX-MM=	Cisco	GE SFP, LC connector SX transceiver	2
PWR-CLIP	PWR-CLIP	Cisco	Power retainer clip for compact switches	2
RCKMNT-19-CMPCT=	RCKMNT-19-CMPCT=	Cisco	19in RackMount for Cisco Catalyst 3560,2960,ME-3400 Compact Switch	2

Small Clinic

Name	Catalog Num	Vendor	Description	Qty
AIR-CAP3502E-A-K9	AIR-CAP3502E-A-K9	Cisco	802.11a/g/n Ctrlr-based AP w/CleanAir; Ext Ant; A Reg Domain	2
AIR-AP-BRACKET-1	AIR-AP-BRACKET-1	Cisco	1040/1140/1260/3500 Low Profile Mounting Bracket (Default)	2
AIR-AP-T-RAIL-R	AIR-AP-T-RAIL-R	Cisco	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	2
AIR-ANT2422DW-R	AIR-ANT2422DW-R	Cisco	2.4 GHz 2.2 dBi Swivel Dipole Antenna White, RP-TNC	6
AIR-ANT5135DW-R	AIR-ANT5135DW-R	Cisco	5 GHz 3.5 dBi Swivel Dipole Antenna White, RP-TNC	6
CON-SNT-CAP3502A	CON-SNT-CAP3502A	Cisco	SMARTNET 8X5XNBD 802.11a/g/n Ctrlr-based AP w/CleanAir; E	2
S3G1RK9W8-12423JA	S3G1RK9W8-12423JA	Cisco	Cisco 3500 Series IOS Wireless LAN Controller-based Recovery	2
AIR-CAP3502I-A-K9	AIR-CAP3502I-A-K9	Cisco	802.11a/g/n Ctrlr-based AP w/CleanAir; Int Ant; A Reg Domain	2
AIR-AP-BRACKET-1	AIR-AP-BRACKET-1	Cisco	1040/1140/1260/3500 Low Profile Mounting Bracket (Default)	2
AIR-AP-T-RAIL-R	AIR-AP-T-RAIL-R	Cisco	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	2

CON-SNT-CAP352IA	CON-SNT-CAP352IA	Cisco	SMARTNET 8X5XNBD 802.11a/g/n Ctrlr-based AP w/CleanAir; I	2
S3G1RK9W8-12423JA	S3G1RK9W8-12423JA	Cisco	Cisco 3500 Series IOS Wireless LAN Controller-based Recovery	2
CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	2
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	2
CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	2
CISCO2921-SEC/K9	CISCO2921-SEC/K9	Cisco	Cisco 2921 Security Bundle w/SEC license PAK	1
CAB-ADSL-RJ11	CAB-ADSL-RJ11	Cisco	Lavender Cable for xDSL, Straight-through, RJ-11, 6 feet	1
ISR-CCP-EXP	ISR-CCP-EXP	Cisco	Cisco Config Pro Express on Router Flash	1
PWR-2921-51-AC	PWR-2921-51-AC	Cisco	Cisco 2921/2951 AC Power Supply	1
SL-29-IPB-K9	SL-29-IPB-K9	Cisco	IP Base License for Cisco 2901-2951	1
SL-29-SEC-K9	SL-29-SEC-K9	Cisco	Security License for Cisco 2901-2951	1
SM-DSK-SATA-500GB	SM-DSK-SATA-500GB	Cisco	500 GB hard disk drive for SRE SM	2
SM-MEM-VLP-2GB	SM-MEM-VLP-2GB	Cisco	2GB Very Low Profile SDRAM for SRE SM	2
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	1
CON-SNT-2921SEC	CON-SNT-2921SEC	Cisco	SMARTNET 8X5XNBD Cisco 2921 Security	1
DISK-MODE-RAID-0	DISK-MODE-RAID-0	Cisco	Configure hard drives as RAID 0	1
FL-VMSS-SM-MS	FL-VMSS-SM-MS	Cisco	Video Management and Storage System Media Server License	1
FL-VMSS-SM-OM	FL-VMSS-SM-OM	Cisco	Video Management and Storage System Operations Manager Licen	1
HWIC-1ADSL	HWIC-1ADSL	Cisco	1-port ADSLoPOTS HWIC	1
HWIC-3G-HSPA-A	HWIC-3G-HSPA-A	Cisco	3G HWIC ATT HSPA/UMTS 850/1900/2100MHz; Quad-band 2G	1
MEM-2900-512U2.5GB	MEM-2900-512U2.5GB	Cisco	512MB to 2.5GB DRAM Upgrade (2GB+512MB) for Cisco 2901-2921	1
MEM-CF-256U2GB	MEM-CF-256U2GB	Cisco	256MB to 2GB Compact Flash Upgrade for Cisco 1900,2900,3900	1
S29UK9-15102T	S29UK9-15102T	Cisco	Cisco 2901-2921 IOS UNIVERSAL	1

SM-SRE-900-K9	SM-SRE-900-K9	Cisco	Services Module with Services Ready Engine (SRE)	1
SM-VMSS-6.2.1-K9	SM-VMSS-6.2.1-K9	Cisco	Video Management and Storage System Software 6.2.1for the SM	1
SM9-VMSS	SM9-VMSS	Cisco	VMSS software contrainer for SM-SRE-900-K9	1
VWIC2-2MFT-T1/E1	VWIC2-2MFT-T1/E1	Cisco	2-Port 2nd Gen Multiflex Trunk Voice/WAN Int. Card - T1/E1	1
CIVS-IPC-2421	CIVS-IPC-2421	Cisco	Cisco Indoor SD IP Dome, 2.8-10mm, D/N, Smoked, CM	1
CON-SNT-IPC2421	CON-SNT-IPC2421	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2421	1
CIVS-IPC-2500	CIVS-IPC-2500	Cisco	Cisco 2500 IP Camera, Full Resolution, Day/Night	1
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	1
CIVS-IPC-VT55	CIVS-IPC-VT55	Cisco	Cisco IP Camera Tamron 5-50mm Varifocal Lens	1
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	1
CON-SNT-IPC2500	CON-SNT-IPC2500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2500	1
CIVS-IPC-2520V	CIVS-IPC-2520V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, VR	1
CON-SNT-IPC2520	CON-SNT-IPC2520	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2520V	1
CIVS-IPC-2521V	CIVS-IPC-2521V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, Smoked, VR	1
CON-SNT-IPC2521	CON-SNT-IPC2521	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2521V	1
CIVS-IPC-4500	CIVS-IPC-4500	Cisco	Cisco 4500 IP Camera, HD, DSP, Day/Night	1
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	1
CIVS-IPC-VFM15-50	CIVS-IPC-VFM15-50	Cisco	Cisco IP Camera Lens Megapixel 15-50mm Fujinon	1
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	1
CON-SNT-IPC4500	CON-SNT-IPC4500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-4500	1
CIVS-IPC-5010	CIVS-IPC-5010	Cisco	Cisco Video Surveillance IP Camera, Indoor HD Dome (Clear)	1
CON-SNT-CIVSIPC1	CON-SNT-CIVSIPC1	Cisco	SMARTNET 8X5XNBD Cisco Video Surveillance IP Camera	1
CIVS-IPC-5011	CIVS-IPC-5011	Cisco	Cisco Video Surveillance IP Camera, Indoor HD Dome (Smoked)	1

CON-SNT-CIVSIPC0	CON-SNT-CIVSIPC0	Cisco	SMARTNET 8X5XNBD Cisco Video Surveillance IP Camera, Indo	1
CIVS-OM-SW4.1=	CIVS-OM-SW4.1=	Cisco	CIVS-OM Operations Manager v4.1 Software Only	1
CON-SAS-OMSW41	CON-SAS-OMSW41	Cisco	SW APP SUPP CIVS-OM Operations Manager v4.1 Software	1
CIVS-VM-1DFL=	CIVS-VM-1DFL=	Cisco	Cisco VS Virtual Matrix Client License, 1 client	1
CON-SAS-VSVMCL1	CON-SAS-VSVMCL1	Cisco	SW APP SUPP CIVS-VM-1DFL	1
CIVS-VM-SW6.2=	CIVS-VM-SW6.2=	Cisco	CIVS-VM Virtual Matrix v6.2 Software License	1
CON-SAS-VMSW62	CON-SAS-VMSW62	Cisco	SW APP SUPP CIVS-VM Virtual Matrix v6.2 Software Lic	1
WS-C2960S-48FPS-L	WS-C2960S-48FPS-L	Cisco	Cisco Catalyst 2960S 48 GigE PoE 740W, 4 x SFP LAN Base	1
CAB-L620P-C13-US	CAB-L620P-C13-US	Cisco	Power Cord, 250VAC, 15A, NEMA L6-20 to C13, US	1

Medium Clinic

Name	Catalog Num	Vendor	Description	Qty
AIR-CAP3502E-A-K9	AIR-CAP3502E-A-K9	Cisco	802.11a/g/n Ctrlr-based AP w/CleanAir; Ext Ant; A Reg Domain	7
AIR-AP-BRACKET-1	AIR-AP-BRACKET-1	Cisco	1040/1140/1260/3500 Low Profile Mounting Bracket (Default)	7
AIR-AP-T-RAIL-R	AIR-AP-T-RAIL-R	Cisco	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	7
AIR-ANT2422DW-R	AIR-ANT2422DW-R	Cisco	2.4 GHz 2.2 dBi Swivel Dipole Antenna White, RP-TNC	21
AIR-ANT5135DW-R	AIR-ANT5135DW-R	Cisco	5 GHz 3.5 dBi Swivel Dipole Antenna White, RP-TNC	21
CON-SNT-CAP3502A	CON-SNT-CAP3502A	Cisco	SMARTNET 8X5XNBD 802.11a/g/n Ctrlr-based AP w/CleanAir; E	7
S3G1RK9W8-12423JA	S3G1RK9W8-12423JA	Cisco	Cisco 3500 Series IOS Wireless LAN Controller-based Recovery	7
AIR-CAP3502I-A-K9	AIR-CAP3502I-A-K9	Cisco	802.11a/g/n Ctrlr-based AP w/CleanAir; Int Ant; A Reg Domain	7
AIR-AP-BRACKET-1	AIR-AP-BRACKET-1	Cisco	1040/1140/1260/3500 Low Profile Mounting Bracket (Default)	7
AIR-AP-T-RAIL-R	AIR-AP-T-RAIL-R	Cisco	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	7

CON-SNT-CAP352IA	CON-SNT-CAP352IA	Cisco	SMARTNET 8X5XNBD 802.11a/g/n Ctrlr-based AP w/CleanAir; I	7
S3G1RK9W8-12423JA	S3G1RK9W8-12423JA	Cisco	Cisco 3500 Series IOS Wireless LAN Controller-based Recovery	7
CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	4
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	4
CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	4
CISCO2951-SEC/K9	CISCO2951-SEC/K9	Cisco	Cisco 2951 Security Bundle w/SEC license PAK	1
CAB-ADSL-RJ11	CAB-ADSL-RJ11	Cisco	Lavender Cable for xDSL, Straight-through, RJ-11, 6 feet	1
ISR-CCP-EXP	ISR-CCP-EXP	Cisco	Cisco Config Pro Express on Router Flash	1
PWR-2921-51-AC	PWR-2921-51-AC	Cisco	Cisco 2921/2951 AC Power Supply	1
SL-29-IPB-K9	SL-29-IPB-K9	Cisco	IP Base License for Cisco 2901-2951	1
SL-29-SEC-K9	SL-29-SEC-K9	Cisco	Security License for Cisco 2901-2951	1
SM-DSK-SATA-500GB	SM-DSK-SATA-500GB	Cisco	500 GB hard disk drive for SRE SM	2
SM-MEM-VLP-2GB	SM-MEM-VLP-2GB	Cisco	2GB Very Low Profile SDRAM for SRE SM	2
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	1
DISK-MODE-RAID-0	DISK-MODE-RAID-0	Cisco	Configure hard drives as RAID 0	1
FL-VMSS-SM-MS	FL-VMSS-SM-MS	Cisco	Video Management and Storage System Media Server License	1
FL-VMSS-SM-OM	FL-VMSS-SM-OM	Cisco	Video Management and Storage System Operations Manager Licen	1
HWIC-1ADSL	HWIC-1ADSL	Cisco	1-port ADSLoPOTS HWIC	1
MEM-2951-512U2GB	MEM-2951-512U2GB	Cisco	512MB to 2GB DRAM Upgrade (1 2GB DIMM) for Cisco 2951 ISR	1
MEM-CF-256U2GB	MEM-CF-256U2GB	Cisco	256MB to 2GB Compact Flash Upgrade for Cisco 1900,2900,3900	1
S2951UK9-15102T	S2951UK9-15102T	Cisco	Cisco 2951 IOS UNIVERSAL	1
SM-SRE-900-K9	SM-SRE-900-K9	Cisco	Services Module with Services Ready Engine (SRE)	1
SM-VMSS-6.2.1-K9	SM-VMSS-6.2.1-K9	Cisco	Video Management and Storage System Software 6.2.1for the SM	1

SM9-VMSS	SM9-VMSS	Cisco	VMSS software contrainer for SM-SRE-900-K9	1
VWIC2-2MFT-T1/E1	VWIC2-2MFT-T1/E1	Cisco	2-Port 2nd Gen Multiflex Trunk Voice/WAN Int. Card - T1/E1	1
CISCO2951-SEC/K9	CISCO2951-SEC/K9	Cisco	Cisco 2951 Security Bundle w/SEC license PAK	1
ISR-CCP-EXP	ISR-CCP-EXP	Cisco	Cisco Config Pro Express on Router Flash	1
PWR-2921-51-AC	PWR-2921-51-AC	Cisco	Cisco 2921/2951 AC Power Supply	1
SL-29-IPB-K9	SL-29-IPB-K9	Cisco	IP Base License for Cisco 2901-2951	1
SL-29-SEC-K9	SL-29-SEC-K9	Cisco	Security License for Cisco 2901-2951	1
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	1
HWIC-3G-HSPA-A	HWIC-3G-HSPA-A	Cisco	3G HWIC ATT HSPA/UMTS 850/1900/2100MHz; Quad-band 2G	1
MEM-2951-512U2GB	MEM-2951-512U2GB	Cisco	512MB to 2GB DRAM Upgrade (1 2GB DIMM) for Cisco 2951 ISR	1
MEM-CF-256U2GB	MEM-CF-256U2GB	Cisco	256MB to 2GB Compact Flash Upgrade for Cisco 1900,2900,3900	1
NME-AIR-WLC25-K9	NME-AIR-WLC25-K9	Cisco	25-AP WLAN Controller NM for Cisco 2800/3800 Series	1
S2951UK9-15102T	S2951UK9-15102T	Cisco	Cisco 2951 IOS UNIVERSAL	1
SM-NM-ADPTR	SM-NM-ADPTR	Cisco	Network Module Adapter for SM Slot on Cisco 2900, 3900 ISR	1
SWLCEK9-60	SWLCEK9-60	Cisco	Cisco Unified WLAN Controller SW Release 6.0 - MD	1
VWIC2-2MFT-T1/E1	VWIC2-2MFT-T1/E1	Cisco	2-Port 2nd Gen Multiflex Trunk Voice/WAN Int. Card - T1/E1	1
CIVS-IPC-2421	CIVS-IPC-2421	Cisco	Cisco Indoor SD IP Dome, 2.8-10mm, D/N, Smoked, CM	2
CON-SNT-IPC2421	CON-SNT-IPC2421	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2421	2
CIVS-IPC-2500	CIVS-IPC-2500	Cisco	Cisco 2500 IP Camera, Full Resolution, Day/Night	2
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	2
CIVS-IPC-VT55	CIVS-IPC-VT55	Cisco	Cisco IP Camera Tamron 5-50mm Varifocal Lens	2
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	2
CON-SNT-IPC2500	CON-SNT-IPC2500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2500	2

CIVS-IPC-2520V	CIVS-IPC-2520V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, VR	2
CON-SNT-IPC2520	CON-SNT-IPC2520	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2520V	2
CIVS-IPC-2521V	CIVS-IPC-2521V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, Smoked, VR	1
CON-SNT-IPC2521	CON-SNT-IPC2521	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2521V	1
CIVS-IPC-2521V	CIVS-IPC-2521V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, Smoked, VR	1
CON-SNT-IPC2521	CON-SNT-IPC2521	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2521V	1
CIVS-IPC-4500	CIVS-IPC-4500	Cisco	Cisco 4500 IP Camera, HD, DSP, Day/Night	2
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	2
CIVS-IPC-VFM15-50	CIVS-IPC-VFM15-50	Cisco	Cisco IP Camera Lens Megapixel 15-50mm Fujinon	2
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	2
CON-SNT-IPC4500	CON-SNT-IPC4500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-4500	2
CIVS-IPC-5010	CIVS-IPC-5010	Cisco	Cisco Video Surveillance IP Camera, Indoor HD Dome (Clear)	2
CON-SNT-CIVSIPC1	CON-SNT-CIVSIPC1	Cisco	SMARTNET 8X5XNBD Cisco Video Surveillance IP Camera	2
CIVS-IPC-5011	CIVS-IPC-5011	Cisco	Cisco Video Surveillance IP Camera, Indoor HD Dome (Smoked)	2
CON-SNT-CIVSIPC0	CON-SNT-CIVSIPC0	Cisco	SMARTNET 8X5XNBD Cisco Video Surveillance IP Camera, Indo	2
CIVS-OM-SW4.1=	CIVS-OM-SW4.1=	Cisco	CIVS-OM Operations Manager v4.1 Software Only	1
CON-SAS-OMSW41	CON-SAS-OMSW41	Cisco	SW APP SUPP CIVS-OM Operations Manager v4.1 Software	1
CIVS-VM-1DFL=	CIVS-VM-1DFL=	Cisco	Cisco VS Virtual Matrix Client License, 1 client	1
CON-SAS-VSVMCL1	CON-SAS-VSVMCL1	Cisco	SW APP SUPP CIVS-VM-1DFL	1
CIVS-VM-SW6.2=	CIVS-VM-SW6.2=	Cisco	CIVS-VM Virtual Matrix v6.2 Software License	1
CON-SAS-VMSW62	CON-SAS-VMSW62	Cisco	SW APP SUPP CIVS-VM Virtual Matrix v6.2 Software Lic	1
WS-C2960PD-8TT-L	WS-C2960PD-8TT-L	Cisco	Cisco Catalyst 2960 Powered Device 8 10/100 + 1 1000BT LAN Base	10
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	10

CON-SNT-C2960P8T	CON-SNT-C2960P8T	Cisco	SMARTNET 8X5XNBD Cat2960 Pwrd Device 8 10/100-1 1K BT LAN	10
PWR-A	PWR-A	Cisco	Pwr Sply In:100-240VAC Out:48VDC 380mA-2960PD-8TT-L	10
WS-C3750X-48PF-S	WS-C3750X-48PF-S	Cisco	Cisco Catalyst 3750X 48 Port Full PoE IP Base	2
C3KX-PWR-1100WAC	C3KX-PWR-1100WAC	Cisco	Cisco Catalyst 3K-X 1100W AC Power Supply	2
C3KX-NM-1G	C3KX-NM-1G	Cisco	Cisco Catalyst 3K-X 1G Network Module option PID	2
C3KX-PWR-1100WAC/2	C3KX-PWR-1100WAC /2	Cisco	Cisco Catalyst 3K-X 1100W AC Secondary Power Supply	2
CAB-3KX-AC	CAB-3KX-AC	Cisco	AC Power Cord for Catalyst 3K-X (North America)	4
CAB-SPWR-150CM	CAB-SPWR-150CM	Cisco	3750X Stack Power Cable 150 CM - Upgrade	2
CAB-STACK-1M-NH	CAB-STACK-1M-NH	Cisco	Cisco StackWise 1M Non-Halogen Lead Free Stacking Cable	2
CON-SNT-3750X4FS	CON-SNT-3750X4FS	Cisco	SMARTNET 8X5XNBD Catalyst 3750X 48 Port Full PoE IP Base	2
S375XVK9T-12253SE	S375XVK9T-12253SE	Cisco	Cisco CAT 3750X IOS UNIVERSAL WITH WEB BASE DEV MGR	2
SFP-GE-S=	SFP-GE-S=	Cisco	1000BASE-SX SFP (DOM)	8

Hospital

Name	Catalog Num	Vendor	Description	Qty
AIR-CAP3502E-A-K9	AIR-CAP3502E-A-K9	Cisco	802.11a/g/n Ctrlr-based AP w/CleanAir; Ext Ant; A Reg Domain	12
AIR-AP-BRACKET-1	AIR-AP-BRACKET-1	Cisco	1040/1140/1260/3500 Low Profile Mounting Bracket (Default)	12
AIR-AP-T-RAIL-R	AIR-AP-T-RAIL-R	Cisco	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	12
AIR-ANT2422DW-R	AIR-ANT2422DW-R	Cisco	2.4 GHz 2.2 dBi Swivel Dipole Antenna White, RP-TNC	36
AIR-ANT5135DW-R	AIR-ANT5135DW-R	Cisco	5 GHz 3.5 dBi Swivel Dipole Antenna White, RP-TNC	36
CON-SNT-CAP3502A	CON-SNT-CAP3502A	Cisco	SMARTNET 8X5XNBD 802.11a/g/n Ctrlr-based AP w/CleanAir; E	12
S3G1RK9W8-12423JA	S3G1RK9W8-12423JA	Cisco	Cisco 3500 Series IOS Wireless LAN Controller-based Recovery	12

AIR-CAP3502I-A-K9	AIR-CAP3502I-A-K9	Cisco	802.11a/g/n Ctrlr-based AP w/CleanAir; Int Ant; A Reg Domain	12
AIR-AP-BRACKET-1	AIR-AP-BRACKET-1	Cisco	1040/1140/1260/3500 Low Profile Mounting Bracket (Default)	12
AIR-AP-T-RAIL-R	AIR-AP-T-RAIL-R	Cisco	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	12
CON-SNT-CAP352IA	CON-SNT-CAP352IA	Cisco	SMARTNET 8X5XNBD 802.11a/g/n Ctrlr-based AP w/CleanAir; I	12
S3G1RK9W8-12423JA	S3G1RK9W8-12423JA	Cisco	Cisco 3500 Series IOS Wireless LAN Controller-based Recovery	12
AIR-CT5508-25-K9	AIR-CT5508-25-K9	Cisco	Cisco 5508 Series Wireless Controller for up to 25 APs	2
LIC-CT5508-25	LIC-CT5508-25	Cisco	25 AP Base license	2
LIC-CT5508-BASE	LIC-CT5508-BASE	Cisco	Base Software License	2
AIR-PWR-5500-AC	AIR-PWR-5500-AC	Cisco	Cisco 5500 Series Wireless Controller Redundant Power Supply	2
AIR-PWR-CORD-NA	AIR-PWR-CORD-NA	Cisco	AIR Line Cord North America	4
CON-SNT-CT0825	CON-SNT-CT0825	Cisco	SMARTNET 8X5XNBD Cisco 5508 Series	2
GLC-T=	GLC-T=	Cisco	1000BASE-T SFP	6
SWC5500K9-70	SWC5500K9-70	Cisco	Cisco Unified Wireless Controller SW Release 7.0	2
CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	8
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	8
CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	8
CISCO3945-SEC/K9	CISCO3945-SEC/K9	Cisco	Cisco 3945 Security Bundle w/SEC license PAK	1
3900-FANASSY	3900-FANASSY	Cisco	Cisco 3925/3945 Fan Assembly (Bezel included)	1
C3900-SPE150/K9	C3900-SPE150/K9	Cisco	Cisco Services Performance Engine 150 for Cisco 3945 ISR	1
ISR-CCP-EXP	ISR-CCP-EXP	Cisco	Cisco Config Pro Express on Router Flash	1
PWR-3900-AC	PWR-3900-AC	Cisco	Cisco 3925/3945 AC Power Supply	1
SL-39-IPB-K9	SL-39-IPB-K9	Cisco	IP Base License for Cisco 3925/3945	1
SL-39-SEC-K9	SL-39-SEC-K9	Cisco	Security License for Cisco 3900 Series	1

CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	2
CON-P2ST-NMEIPSK9	CON-P2ST-NMEIPSK9	Cisco	PM2, 8X5XNBD NME-IPS-K9	1
CON-SNT-3945SEC	CON-SNT-3945SEC	Cisco	SMARTNET 8X5XNBD Cisco 3945 Security Bundle w/SEC license	1
HWIC-3G-HSPA-A	HWIC-3G-HSPA-A	Cisco	3G HWIC ATT HSPA/UMTS 850/1900/2100MHz; Quad-band 2G	1
IPS-SW-NME-7.0-K9	IPS-SW-NME-7.0-K9	Cisco	IPS Software v7.0 for NME-IPS	1
MEM-3900-1GU2GB	MEM-3900-1GU2GB	Cisco	1GB to 2GB DRAM Upgrade (1GB+1GB) for Cisco 3925/3945 ISR	1
MEM-CF-256U2GB	MEM-CF-256U2GB	Cisco	256MB to 2GB Compact Flash Upgrade for Cisco 1900,2900,3900	1
NME-IPS-K9	NME-IPS-K9	Cisco	Cisco IPS NM for 2811, 2821, 2851 and 3800	1
PWR-3900-AC/2	PWR-3900-AC/2	Cisco	Cisco 3925/3945 AC Power Supply (Secondary PS)	1
S39UK9-15102T	S39UK9-15102T	Cisco	Cisco 3925-3945 IOS UNIVERSAL	1
SM-NM-ADPTR	SM-NM-ADPTR	Cisco	Network Module Adapter for SM Slot on Cisco 2900, 3900 ISR	1
VWIC2-2MFT-T1/E1	VWIC2-2MFT-T1/E1	Cisco	2-Port 2nd Gen Multiflex Trunk Voice/WAN Int. Card - T1/E1	1
CISCO3945-SEC/K9	CISCO3945-SEC/K9	Cisco	Cisco 3945 Security Bundle w/SEC license PAK	1
3900-FANASSY	3900-FANASSY	Cisco	Cisco 3925/3945 Fan Assembly (Bezel included)	1
C3900-SPE150/K9	C3900-SPE150/K9	Cisco	Cisco Services Performance Engine 150 for Cisco 3945 ISR	1
CAB-ADSL-RJ11	CAB-ADSL-RJ11	Cisco	Lavender Cable for xDSL, Straight-through, RJ-11, 6 feet	1
ISR-CCP-EXP	ISR-CCP-EXP	Cisco	Cisco Config Pro Express on Router Flash	1
PWR-3900-AC	PWR-3900-AC	Cisco	Cisco 3925/3945 AC Power Supply	1
SL-39-IPB-K9	SL-39-IPB-K9	Cisco	IP Base License for Cisco 3925/3945	1
SL-39-SEC-K9	SL-39-SEC-K9	Cisco	Security License for Cisco 3900 Series	1
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	2
CON-P2ST-NMEIPSK9	CON-P2ST-NMEIPSK9	Cisco	PM2, 8X5XNBD NME-IPS-K9	1
CON-SNT-3945SEC	CON-SNT-3945SEC	Cisco	SMARTNET 8X5XNBD Cisco 3945 Security Bundle w/SEC license	1

HWIC-1ADSL	HWIC-1ADSL	Cisco	1-port ADSLoPOTS HWIC	1
IPS-SW-NME-7.0-K9	IPS-SW-NME-7.0-K9	Cisco	IPS Software v7.0 for NME-IPS	1
MEM-3900-1GU2GB	MEM-3900-1GU2GB	Cisco	1GB to 2GB DRAM Upgrade (1GB+1GB) for Cisco 3925/3945 ISR	1
MEM-CF-256U2GB	MEM-CF-256U2GB	Cisco	256MB to 2GB Compact Flash Upgrade for Cisco 1900,2900,3900	1
NME-IPS-K9	NME-IPS-K9	Cisco	Cisco IPS NM for 2811, 2821, 2851 and 3800	1
PWR-3900-AC/2	PWR-3900-AC/2	Cisco	Cisco 3925/3945 AC Power Supply (Secondary PS)	1
S39UK9-15102T	S39UK9-15102T	Cisco	Cisco 3925-3945 IOS UNIVERSAL	1
SM-NM-ADPTR	SM-NM-ADPTR	Cisco	Network Module Adapter for SM Slot on Cisco 2900, 3900 ISR	1
VWIC2-2MFT-T1/E1	VWIC2-2MFT-T1/E1	Cisco	2-Port 2nd Gen Multiflex Trunk Voice/WAN Int. Card - T1/E1	1
CIVS-IPC-2421	CIVS-IPC-2421	Cisco	Cisco Indoor SD IP Dome, 2.8-10mm, D/N, Smoked, CM	4
CON-SNT-IPC2421	CON-SNT-IPC2421	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2421	4
CIVS-IPC-2500	CIVS-IPC-2500	Cisco	Cisco 2500 IP Camera, Full Resolution, Day/Night	4
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	4
CIVS-IPC-VT55	CIVS-IPC-VT55	Cisco	Cisco IP Camera Tamron 5-50mm Varifocal Lens	4
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	4
CON-SNT-IPC2500	CON-SNT-IPC2500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2500	4
CIVS-IPC-2520V	CIVS-IPC-2520V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, VR	4
CON-SNT-IPC2520	CON-SNT-IPC2520	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2520V	4
CIVS-IPC-2521V	CIVS-IPC-2521V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, Smoked, VR	4
CON-SNT-IPC2521	CON-SNT-IPC2521	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2521V	4
CIVS-IPC-4500	CIVS-IPC-4500	Cisco	Cisco 4500 IP Camera, HD, DSP, Day/Night	4
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	4
CIVS-IPC-VFM15-50	CIVS-IPC-VFM15-50	Cisco	Cisco IP Camera Lens Megapixel 15-50mm Fujinon	4

CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	4
CON-SNT-IPC4500	CON-SNT-IPC4500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-4500	4
CIVS-IPC-5010	CIVS-IPC-5010	Cisco	Cisco Video Surveillance IP Camera, Indoor HD Dome (Clear)	4
CON-SNT-CIVSIPC1	CON-SNT-CIVSIPC1	Cisco	SMARTNET 8X5XNBD Cisco Video Surveillance IP Camera	4
CIVS-IPC-5011	CIVS-IPC-5011	Cisco	Cisco Video Surveillance IP Camera, Indoor HD Dome (Smoked)	4
CON-SNT-CIVSIPC0	CON-SNT-CIVSIPC0	Cisco	SMARTNET 8X5XNBD Cisco Video Surveillance IP Camera, Indo	4
CIVS-MSP-2RU	CIVS-MSP-2RU	Cisco	2RU w/Motherboard;1 CPU;RAID;Pwr Supp;NO Drives;NO Options	1
CIVS-CAB-16-AC	CIVS-CAB-16-AC	Cisco	CIVS C16 Power Cable North America	2
CIVS-HDD-1000	CIVS-HDD-1000	Cisco	1TB SATA Drive for CIVS-MSP	12
CIVS-MS-SW6.2	CIVS-MS-SW6.2	Cisco	CIVS-MS Media Server v6.2 Software License with Hardware	1
CIVS-PS-900	CIVS-PS-900	Cisco	Redundant 900W Power Supply for CIVS-MSP 2RU, 4RU	1
CIVS-VSM-SW4262	CIVS-VSM-SW4262	Cisco	CIVS-VSM Video Surveillance Manager v4.2/6.2 SW Mfg Image	1
CON-SNT-VSM2U	CON-SNT-VSM2U	Cisco	SMARTNET 8X5XNBD 2RU MSP Assembly	1
CIVS-OM-SW4.1=	CIVS-OM-SW4.1=	Cisco	CIVS-OM Operations Manager v4.1 Software Only	1
CON-SAS-OMSW41	CON-SAS-OMSW41	Cisco	SW APP SUPP CIVS-OM Operations Manager v4.1 Software	1
CIVS-VM-1DFL=	CIVS-VM-1DFL=	Cisco	Cisco VS Virtual Matrix Client License, 1 client	2
CON-SAS-VSVMCL1	CON-SAS-VSVMCL1	Cisco	SW APP SUPP CIVS-VM-1DFL	2
CIVS-VM-SW6.2=	CIVS-VM-SW6.2=	Cisco	CIVS-VM Virtual Matrix v6.2 Software License	1
CON-SAS-VMSW62	CON-SAS-VMSW62	Cisco	SW APP SUPP CIVS-VM Virtual Matrix v6.2 Software Lic	1
WS-C3560-8PC-S	WS-C3560-8PC-S	Cisco	Catalyst 3560 Compact 8 10/100 PoE + 1 T/SFP; IP Base Image	20
CAB-AC-RA	CAB-AC-RA	Cisco	Power Cord,110V, Right Angle	20
CON-SNTP-WSC3568	CON-SNTP-WSC3568	Cisco	SMARTNET 24X7X4 Catalyst 3560 8 10/1	20
WS-C3560X-24P-S	WS-C3560X-24P-S	Cisco	Cisco Catalyst 3560X 24 Port PoE IP Base	6

C3KX-PWR-715WAC	C3KX-PWR-715WAC	Cisco	Cisco Catalyst 3K-X 715W AC Power Supply	6
C3KX-NM-1G	C3KX-NM-1G	Cisco	Cisco Catalyst 3K-X 1G Network Module option PID	6
CAB-3KX-AC	CAB-3KX-AC	Cisco	AC Power Cord for Catalyst 3K-X (North America)	6
CON-SNT-3560X2PS	CON-SNT-3560X2PS	Cisco	SMARTNET 8X5XNBD Catalyst 3560X 24 Port PoE IP Base	6
S356XVK9T-12253SE	S356XVK9T-12253SE	Cisco	CAT 3560X IOS UNIVERSAL WITH WEB BASED DEV MGR	6
SFP-GE-S=	SFP-GE-S=	Cisco	1000BASE-SX SFP (DOM)	12
WS-C4507R+E	WS-C4507R+E	Cisco	Cisco Catalyst 4500E 7 slot chassis for 48Gbps/slot	2
C4500E-IPB	C4500E-IPB	Cisco	Paper IP Base License	2
CAB-AC-2800W-TWLK	CAB-AC-2800W-TWLK	Cisco	U.S. Power Cord, Twist Lock, NEMA 6-20 Plug	4
CON-SNT-C4507R+E	CON-SNT-C4507R+E	Cisco	SMARTNET 8X5XNBD Catalyst4500E 7 slot chassis for 48Gbps	2
GLC-SX-MM=	GLC-SX-MM=	Cisco	GE SFP, LC connector SX transceiver	48
PWR-C45-2800ACV	PWR-C45-2800ACV	Cisco	Cisco Catalyst 4500 2800W AC Power Supply (Data and PoE)	2
PWR-C45-2800ACV/2	PWR-C45-2800ACV/2	Cisco	Cisco Catalyst 4500 2800W AC Power Supply (Data and PoE)	2
S45UK9-31-01XO	S45UK9-31-01XO	Cisco	CAT4500e SUP7e Universal Crypto Image	2
WS-X4448-GB-SFP	WS-X4448-GB-SFP	Cisco	Cisco Catalyst 4500 48-Port 1000Base-X (SFPs Optional)	2
WS-X45-SUP7-E	WS-X45-SUP7-E	Cisco	Cisco Catalyst 4500 E-Series Supervisor, 848Gbps	2
WS-X45-SUP7-E/2	WS-X45-SUP7-E/2	Cisco	Cisco Catalyst 4500 E-Series Supervisor, 848Gbps	2
WS-X4624-SFP-E	WS-X4624-SFP-E	Cisco	Cisco Catalyst 4500 E-Series 24-Port GE (SFP)	2
WS-X4748-RJ45V+E	WS-X4748-RJ45V+E	Cisco	Cisco Catalyst 4500E 48-Port PoE 802.3at 10/100/1000(RJ45)	2

Data Center, Internet Edge, DMZ

Name	Catalog Num	Vendor	Description	Qty
ASA5585-S60-2A-K9	ASA5585-S60-2A-K9	Cisco	Cisco ASA 5585-X Chas w/ SSP60,6 GE,4 SFP+,2 GE Mgt,2 AC,3DES/AES	2
ASA-SSP-60-INC	ASA-SSP-60-INC	Cisco	Cisco ASA 5585-X Security Services Processor-60 with 6GE, 4SFP+	2
ASA-VPN-CLNT-K9	ASA-VPN-CLNT-K9	Cisco	Cisco VPN Client Software (Windows, Solaris, Linux, Mac)	2
ASA5500-ENCR-K9	ASA5500-ENCR-K9	Cisco	Cisco ASA 5500 Strong Encryption License (3DES/AES)	2
ASA5585-BLANK-F	ASA5585-BLANK-F	Cisco	Cisco ASA 5585-X Full Width Blank Slot Cover	2
ASA5585-BLANK-HD	ASA5585-BLANK-HD	Cisco	Cisco ASA 5585-X Hard Drive Blank Slot Cover	4
ASA5585-PWR-AC	ASA5585-PWR-AC	Cisco	Cisco ASA 5585-X AC Power Supply	4
ASA-ADV-END-SEC	ASA-ADV-END-SEC	Cisco	Cisco ASA 5500 Advanced Endpoint Assessment License for SSL VPN	2
ASA5500-SC-10	ASA5500-SC-10	Cisco	Cisco ASA 5500 10 Security Contexts License	2
ASA5500-SSL-1000	ASA5500-SSL-1000	Cisco	Cisco ASA 5500 SSL VPN 1000 Premium User License	2
CAB-US515P-C19-US	CAB-US515P-C19-US	Cisco	NEMA 5-15 to IEC-C19 13ft US	4
CON-SNT-A85S62K9	CON-SNT-A85S62K9	Cisco	SMARTNET 8X5XNBD ASA 5585-X Chas w/ SSP40,6 GE,4 SFP+,2 G	2
SF-ASA5585-8.2-K8	SF-ASA5585-8.2-K8	Cisco	Cisco ASA 5500 Series Software Version 8.2 for ASA 5585-X, DES	2
ASR1002-5G-SHA/K9	ASR1002-5G-SHA/K9	Cisco	Cisco ASR1002 Sec+HA Bundle w/ ESP-5G,AESK9,License,4GB DRAM	2
ASR1000-ESP5	ASR1000-ESP5	Cisco	Cisco ASR1K Embedded Services Processor,5Gbps,ASR1002 only	2
FLASR1-FPI-RTU	FLASR1-FPI-RTU	Cisco	Flex. Pack Insp. Right-To-Use Feat Lic,ASR1000 Series	2
FLASR1-FW-RTU	FLASR1-FW-RTU	Cisco	Firewall Right-To-Use Feature Lic for ASR1000 Series	2
FLASR1-IOSRED-RTU	FLASR1-IOSRED-RTU	Cisco	SW Redundancy Right-To-Use Feat Lic for ASR1000 Series	2
FLASR1-IPSEC-RTU	FLASR1-IPSEC-RTU	Cisco	Encryption Right-To-Use Feature Lic for ASR1000 Series	2
SASR1R1-AESK9-31S	SASR1R1-AESK9-31S	Cisco	Cisco ASR 1000 Series RP1 ADVANCED ENTERPRISE SERVICES	2
ASR1002-PWR-AC	ASR1002-PWR-AC	Cisco	Cisco ASR1002 AC Power Supply	4

CAB-AC-RA	CAB-AC-RA	Cisco	Power Cord,110V, Right Angle	4
CON-SNTP-25GSHAK9	CON-SNTP-25GSHAK 9	Cisco	SMARTNET 24X7X4 ASR1002 Sec+HA Bundle w/ESP-5G, AESK9	2
ASR1004-20G-HA/K9	ASR1004-20G-HA/K9	Cisco	Cisco ASR1004 HA Bundle w/ ESP-20G,RP1,SIP10,AESK9,License	2
ASR1000-ESP20	ASR1000-ESP20	Cisco	Cisco ASR1000 Embedded Services Processor, 20G	2
ASR1000-SPA	ASR1000-SPA	Cisco	SPA for ASR1000; No Physical Part; For Tracking Only	4
FLASR1-IOSRED-RTU	FLASR1-IOSRED-RT U	Cisco	SW Redundancy Right-To-Use Feat Lic for ASR1000 Series	2
M-ASR1K-HDD-40GB	M-ASR1K-HDD-40GB	Cisco	Cisco ASR1000 RP1 40GB HDD	2
M-ASR1K-RP1-4GB	M-ASR1K-RP1-4GB	Cisco	Cisco ASR1000 RP1 4GB DRAM	2
SASR1R1-AESK9-31S	SASR1R1-AESK9-31S	Cisco	Cisco ASR 1000 Series RP1 ADVANCED ENTERPRISE SERVICES	2
ASR1000-RP1-BUN	ASR1000-RP1-BUN	Cisco	Cisco ASR1000 Route Processor 1, 4GB DRAM,Bundle Component	2
ASR1000-SIP10	ASR1000-SIP10	Cisco	Cisco ASR1000 SPA Interface Processor 10	2
ASR1000-SIP10-BUN	ASR1000-SIP10-BUN	Cisco	Cisco ASR1000 SPA Interface Processor 10, Bundle Component	2
ASR1004-PWR-AC	ASR1004-PWR-AC	Cisco	Cisco ASR1004 AC Power Supply	4
CAB-AC15A-90L-US	CAB-AC15A-90L-US	Cisco	15A AC Pwr Cord, left-angle (United States) (bundle option)	4
CON-SNTP-420GHAK9	CON-SNTP-420GHAK 9	Cisco	SMARTNET 24X7X4 ASR1004 Chassis 2 P/S	2
CON-SNTP-A1ESP20	CON-SNTP-A1ESP20	Cisco	SMARTNET 24X7X4 ASR1000 Embedded Svc Processor,20G,Crypt	2
CON-SNTP-ASRRP1B	CON-SNTP-ASRRP1B	Cisco	SMARTNET 24X7X4 Cisco ASR1000 Route Processor 1	2
CON-SNTP-ASRSIPB	CON-SNTP-ASRSIPB	Cisco	SMARTNET 24X7X4 Cisco ASR1000 SPA Interface Processor	2
FLASR1-FW-RTU	FLASR1-FW-RTU	Cisco	Firewall Right-To-Use Feature Lic for ASR1000 Series	2
SPA-1X10GE-L-V2	SPA-1X10GE-L-V2	Cisco	Cisco 1-Port 10GE LAN-PHY Shared Port Adapter	4
XFP-10G-MM-SR	XFP-10G-MM-SR	Cisco	10GBASE-SR XFP Module	4
CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	4
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	4

CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	4
CIVS-IPC-2520V	CIVS-IPC-2520V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, VR	4
CON-SNT-IPC2520	CON-SNT-IPC2520	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2520V	4
Ironport Bundle E-mail and Web	Ironport Bundle E-mail and Web	Cisco	Ironport A La Carte examples for Webn and E-mail	2
N5K-C5020P-NBF	N5K-C5020P-NBF	Cisco	Cisco Nexus 5020 NetApp OSM version, 2 PS	2
N5020-ACC-KIT	N5020-ACC-KIT	Cisco	Cisco Nexus 5020 Accessory Kit, Option	2
N5K-PAC-1200W	N5K-PAC-1200W	Cisco	Cisco Nexus 5020 PSU module, 100-240VAC 1200W	4
CAB-9K12A-NA	CAB-9K12A-NA	Cisco	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	4
CON-SNTP-N5020	CON-SNTP-N5020	Cisco	SMARTNET 24X7X4 N5000 2RU Chassis no PS 5	2
N5000FMS1K9	N5000FMS1K9	Cisco	Cisco Nexus 5000 Fabric Manager Server License	2
N5K-M1600	N5K-M1600	Cisco	N5000 1000 Series Module 6port 10GE(req SFP+)	4
N5KUK9-421N2.1	N5KUK9-421N2.1	Cisco	Cisco Nexus 5000 Base OS Software Rel 4.2(1)N2(1)	2
SFP-H10GB-CU1M	SFP-H10GB-CU1M	Cisco	10GBASE-CU SFP+ Cable 1 Meter	16
SFP-H10GB-CU3M	SFP-H10GB-CU3M	Cisco	10GBASE-CU SFP+ Cable 3 Meter	64
WS-C3750X-24T-S	WS-C3750X-24T-S	Cisco	Cisco Catalyst 3750X 24 Port Data IP Base	6
C3KX-PWR-350WAC	C3KX-PWR-350WAC	Cisco	Cisco Catalyst 3K-X 350W AC Power Supply	6
S375XVK9T-12255SE	S375XVK9T-12255SE	Cisco	CAT 3750X IOS UNIVERSAL WITH WEB BASE DEV MGR	6
C3KX-PWR-350WAC/2	C3KX-PWR-350WAC/2	Cisco	Cisco Catalyst 3K-X 350W AC Secondary Power Supply	6
CAB-3KX-AC	CAB-3KX-AC	Cisco	AC Power Cord for Catalyst 3K-X (North America)	12
CAB-SPWR-150CM	CAB-SPWR-150CM	Cisco	3750X Stack Power Cable 150 CM - Upgrade	6
CAB-STACK-1M-NH	CAB-STACK-1M-NH	Cisco	Cisco StackWise 1M Non-Halogen Lead Free Stacking Cable	6
CON-SNTP-3750X2TS	CON-SNTP-3750X2TS	Cisco	SMARTNET 24X7X4 Catalyst 3750X 24 Port Data IP Base	6
WS-C6509-E	WS-C6509-E	Cisco	Cisco Catalyst 6500 Enhanced 9-slot chassis,15RU,no PS,no Fan Tray	1

BF-S720-64MB-RP	BF-S720-64MB-RP	Cisco	Bootflash for SUP720-64MB-RP	2
MEM-C6K-CPTFL1GB	MEM-C6K-CPTFL1GB	Cisco	Cisco Catalyst 6500 Compact Flash Memory 1GB	2
MEM-XCEF720-256M	MEM-XCEF720-256M	Cisco	Cisco Catalyst 6500 256MB DDR, xCEF720 (67xx interface, DFC3A)	1
WS-SVC-ASA-SM1-K9	WS-SVC-ASA-SM1-K9	Cisco	ASA Services Module for Catalyst 6500-E, 3DES/AES	1
SF-ASASM-8.5-K8	SF-ASASM-8.5-K8	Cisco	ASA Software 8.5 for Catalyst 6500-E ASASM, 2 free VFW	1
MEM-C6K-APP-24GB	MEM-C6K-APP-24GB	Cisco	Cat6500 24GB Service Module Memory	1
WS-SVC-ASA-SM1	WS-SVC-ASA-SM1	Cisco	Base ASA Services Module PID for K8/K9	1
SF-ASASM-ASDM-6.5	SF-ASASM-ASDM-6.5	Cisco	ASDM Software 6.5 for Catalyst 6500-E ASASM	1
ASA5500-ENCR-K9	ASA5500-ENCR-K9	Cisco	ASA 5500 Strong Encryption License (3DES/AES)	1
CON-OSP-ASASM9	CON-OSP-ASASM9	Cisco	ONSITE 24X7X4 ASA Service Module for Catalyst 6500-E	1
VS-F6K-MSFC3	VS-F6K-MSFC3	Cisco	Cisco Catalyst 6500 Multilayer Switch Feature Card (MSFC) III	2
VS-F6K-PFC3C	VS-F6K-PFC3C	Cisco	Cisco Catalyst 6500 Sup 720-10G Policy Feature Card 3C	2
VS-S720-10G	VS-S720-10G	Cisco	Cisco Catalyst 6500 Supervisor 720 with 2 10GbE ports	2
WS-F6700-CFC	WS-F6700-CFC	Cisco	Cisco Catalyst 6500 Central Fwd Card for WS-X67xx modules	1
WS-F6700-DFC3CXL	WS-F6700-DFC3CXL	Cisco	Cisco Catalyst 6500 Dist Fwd Card- 3CXL, for WS-X67xx	1
WS-X6716-10GE	WS-X6716-10GE	Cisco	Cisco Catalyst 6500 16 port 10 Gigabit Ethernet Base Module	1
ACE30-MOD-K9	ACE30-MOD-K9	Cisco	Application Control Engine 30 Hardware	1
SC6K-A51-ACE	SC6K-A51-ACE	Cisco	ACE30 module Software Release 5(1)	1
ACE30-BASE-04-K9	ACE30-BASE-04-K9	Cisco	ACE30 Module with 4G, 1G Comp, 1K SSL TPS and 5VC	1
CON-OSP-ACE30MOD	CON-OSP-ACE30MOD	Cisco	ONSITE 24X7X4 Application Control Engine 30 Hardware	1
CAB-AC-C6K-TWLK	CAB-AC-C6K-TWLK	Cisco	Power Cord, 250Vac 16A, twist lock NEMA L6-20 plug, US	4
CF-ADAPTER-SP	CF-ADAPTER-SP	Cisco	SP adapter for SUP720 and SUP720-10G	2
CON-P2OS-WIDSBNK9	CON-P2OS-WIDSBNK9	Cisco	PM2,OS 8X5XNBD 600M IDSM-2 Mod for	1

MEM-C6K-CPTFL1GB	MEM-C6K-CPTFL1GB	Cisco	Cisco Catalyst 6500 Compact Flash Memory 1GB	2
WS-SVC-ASA-SM1-K9	WS-SVC-ASA-SM1-K9	Cisco	ASA Services Module for Catalyst 6500-E, 3DES/AES	1
SF-ASASM-8.5-K8	SF-ASASM-8.5-K8	Cisco	ASA Software 8.5 for Catalyst 6500-E ASASM, 2 free VFW	1
MEM-C6K-APP-24GB	MEM-C6K-APP-24GB	Cisco	Cat6500 24GB Service Module Memory	1
WS-SVC-ASA-SM1	WS-SVC-ASA-SM1	Cisco	Base ASA Services Module PID for K8/K9	1
SF-ASASM-ASDM-6.5	SF-ASASM-ASDM-6.5	Cisco	ASDM Software 6.5 for Catalyst 6500-E ASASM	1
ASA5500-ENCR-K9	ASA5500-ENCR-K9	Cisco	ASA 5500 Strong Encryption License (3DES/AES)	1
CON-OSP-ASASM9	CON-OSP-ASASM9	Cisco	ONSITE 24X7X4 ASA Service Module for Catalyst 6500-E	1
SC-SVC-IPSV7.0-K9	SC-SVC-IPSV7.0-K9	Cisco	IPS Software v7.0 for IDSM2	1
SV33ISK9C-12233SXI	SV33ISK9C-12233SXI	Cisco	Cisco CAT6000-VSS720 IOS IP SERVICES SSH - DEFAULT	1
VS-S720-10G-3C	VS-S720-10G-3C	Cisco	Cisco Cat 6500 Supervisor 720 with 2 ports 10GbE and MSFC3 PFC3C	2
WS-C6509-E-FAN	WS-C6509-E-FAN	Cisco	Cisco Catalyst 6509-E Chassis Fan Tray	1
WS-CAC-6000W	WS-CAC-6000W	Cisco	Cat6500 6000W AC Power Supply	2
WS-SVC-ASA-SM1-K9	WS-SVC-ASA-SM1-K9	Cisco	ASA Services Module for Catalyst 6500-E, 3DES/AES	1
SF-ASASM-8.5-K8	SF-ASASM-8.5-K8	Cisco	ASA Software 8.5 for Catalyst 6500-E ASASM, 2 free VFW	1
MEM-C6K-APP-24GB	MEM-C6K-APP-24GB	Cisco	Cat6500 24GB Service Module Memory	1
WS-SVC-ASA-SM1	WS-SVC-ASA-SM1	Cisco	Base ASA Services Module PID for K8/K9	1
SF-ASASM-ASDM-6.5	SF-ASASM-ASDM-6.5	Cisco	ASDM Software 6.5 for Catalyst 6500-E ASASM	1
ASA5500-ENCR-K9	ASA5500-ENCR-K9	Cisco	ASA 5500 Strong Encryption License (3DES/AES)	1
CON-OSP-ASASM9	CON-OSP-ASASM9	Cisco	ONSITE 24X7X4 ASA Service Module for Catalyst 6500-E	1
WS-SVC-IDS2-BUN-K9	WS-SVC-IDS2-BUN-K9	Cisco	600M IDSM-2 Mod for Cat	1
WS-X6716-10G-3CXL	WS-X6716-10G-3CXL	Cisco	Cisco Catalyst 6500 16 port 10 Gigabit Ethernet w/ DFC3CXL(req X2)	1
WS-X6748-GE-TX	WS-X6748-GE-TX	Cisco	Cat6500 48-port 10/100/1000 GE Mod: fabric enabled, RJ-45	1

X2-10GB-SR	X2-10GB-SR	Cisco	10GBASE-SR X2 Module	18
WS-C6509-E	WS-C6509-E	Cisco	Cisco Catalyst 6500 Enhanced 9-slot chassis,15RU,no PS,no Fan Tray	1
BF-S720-64MB-RP	BF-S720-64MB-RP	Cisco	Bootflash for SUP720-64MB-RP	2
MEM-C6K-CPTFL1GB	MEM-C6K-CPTFL1GB	Cisco	Cisco Catalyst 6500 Compact Flash Memory 1GB	2
MEM-XCEF720-256M	MEM-XCEF720-256M	Cisco	Cisco Catalyst 6500 256MB DDR, xCEF720 (67xx interface, DFC3A)	1
WS-SVC-ASA-SM1-K9	WS-SVC-ASA-SM1-K9	Cisco	ASA Services Module for Catalyst 6500-E, 3DES/AES	1
SF-ASASM-8.5-K8	SF-ASASM-8.5-K8	Cisco	ASA Software 8.5 for Catalyst 6500-E ASASM, 2 free VFW	1
MEM-C6K-APP-24GB	MEM-C6K-APP-24GB	Cisco	Cat6500 24GB Service Module Memory	1
WS-SVC-ASA-SM1	WS-SVC-ASA-SM1	Cisco	Base ASA Services Module PID for K8/K9	1
SF-ASASM-ASDM-6.5	SF-ASASM-ASDM-6.5	Cisco	ASDM Software 6.5 for Catalyst 6500-E ASASM	1
ASA5500-ENCR-K9	ASA5500-ENCR-K9	Cisco	ASA 5500 Strong Encryption License (3DES/AES)	1
CON-OSP-ASASM9	CON-OSP-ASASM9	Cisco	ONSITE 24X7X4 ASA Service Module for Catalyst 6500-E	1
VS-F6K-MSFC3	VS-F6K-MSFC3	Cisco	Cisco Catalyst 6500 Multilayer Switch Feature Card (MSFC) III	2
VS-F6K-PFC3C	VS-F6K-PFC3C	Cisco	Cisco Catalyst 6500 Sup 720-10G Policy Feature Card 3C	2
VS-S720-10G	VS-S720-10G	Cisco	Cisco Catalyst 6500 Supervisor 720 with 2 10GbE ports	2
WS-F6700-CFC	WS-F6700-CFC	Cisco	Cisco Catalyst 6500 Central Fwd Card for WS-X67xx modules	1
WS-F6700-DFC3CXL	WS-F6700-DFC3CXL	Cisco	Cisco Catalyst 6500 Dist Fwd Card- 3CXL, for WS-X67xx	1
WS-X6716-10GE	WS-X6716-10GE	Cisco	Cisco Catalyst 6500 16 port 10 Gigabit Ethernet Base Module	1
ACE30-MOD-K9	ACE30-MOD-K9	Cisco	Application Control Engine 30 Hardware	1
SC6K-A51-ACE	SC6K-A51-ACE	Cisco	ACE30 module Software Release 5(1)	1
ACE30-BASE-04-K9	ACE30-BASE-04-K9	Cisco	ACE30 Module with 4G, 1G Comp, 1K SSL TPS and 5VC	1
CON-OSP-ACE30MOD	CON-OSP-ACE30MOD	Cisco	ONSITE 24X7X4 Application Control Engine 30 Hardware	1
CAB-AC-C6K-TWLK	CAB-AC-C6K-TWLK	Cisco	Power Cord, 250Vac 16A, twist lock NEMA L6-20 plug, US	4

CF-ADAPTER-SP	CF-ADAPTER-SP	Cisco	SP adapter for SUP720 and SUP720-10G	2
CON-P2OS-WIDSBNK9	CON-P2OS-WIDSBNK 9	Cisco	PM2,OS 8X5XNBD 600M IDSM-2 Mod for	1
MEM-C6K-CPTFL1GB	MEM-C6K-CPTFL1GB	Cisco	Cisco Catalyst 6500 Compact Flash Memory 1GB	2
SC-SVC-IPSV7.0-K9	SC-SVC-IPSV7.0-K9	Cisco	IPS Software v7.0 for IDSM2	1
SV33ISK9C-12233SXI	SV33ISK9C-12233SXI	Cisco	Cisco CAT6000-VSS720 IOS IP SERVICES SSH - DEFAULT	1
VS-S720-10G-3C	VS-S720-10G-3C	Cisco	Cat 6500 Supervisor 720 with 2 ports 10GbE and MSFC3 PFC3C	2
WS-C6509-E-FAN	WS-C6509-E-FAN	Cisco	Cisco Catalyst 6509-E Chassis Fan Tray	1
WS-CAC-6000W	WS-CAC-6000W	Cisco	Cat6500 6000W AC Power Supply	2
WS-SVC-IDS2-BUN-K9	WS-SVC-IDS2-BUN-K 9	Cisco	600M IDSM-2 Mod for Cat	1
WS-X6716-10G-3CXL	WS-X6716-10G-3CXL	Cisco	Cisco Catalyst 6500 16 port 10 Gigabit Ethernet w/ DFC3CXL(req X2)	1
WS-X6748-GE-TX	WS-X6748-GE-TX	Cisco	Cat6500 48-port 10/100/1000 GE Mod: fabric enabled, RJ-45	1
X2-10GB-SR	X2-10GB-SR	Cisco	10GBASE-SR X2 Module	18

Data Center—WAN Aggregation

Name	Catalog Num	Vendor	Description	Qty
ASA5555-IPS-K9	ASA5555-IPS-K9	Cisco	ASA 5555-X with IPS, SW, 8GE Data, 1GE Mgmt, AC, 3DES/AES	1
ASA5500-SSL-10	ASA5500-SSL-10	Cisco	ASA 5500 SSL VPN 10 Premium User License	1
ASA-ADV-END-SEC	ASA-ADV-END-SEC	Cisco	ASA 5500 Advanced Endpoint Assessment License for SSL VPN	1
ASA-AC-E-5555	ASA-AC-E-5555	Cisco	AnyConnect Essentials VPN License - ASA 5555-X (5000 Users)	1
ASA-VPNP-5555	ASA-VPNP-5555	Cisco	Premium Shared VPN Participant License - ASA 5555-X	1
ASA-AC-M-5555	ASA-AC-M-5555	Cisco	AnyConnect Mobile - ASA 5555-X (req. Essentials or Premium)	1
ASA5500-SC-5	ASA5500-SC-5	Cisco	ASA 5500 5 Security Contexts License	1

CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	1
SF-ASA-9.1-K8	SF-ASA-9.1-K8	Cisco	ASA 5500 Series Software Ver. 9.1 for ASA 5512X--5555X, DES	1
SF-ASAIPS64-7.1-K9	SF-ASAIPS64-7.1-K9	Cisco	ASA 5500-X IPS Software 7.1 for IPS SSP	1
ASA5555-IPS-SSP	ASA5555-IPS-SSP	Cisco	ASA 5555-X IPS SSP License	1
ASA-PWR-AC	ASA-PWR-AC	Cisco	ASA 5545-X/5555-X AC Power Supply	1
ASA-PWR-BLANK	ASA-PWR-BLANK	Cisco	ASA 5545-X/5555-X Power Slot Blank Cover	1
ASA5500-ENCR-K9	ASA5500-ENCR-K9	Cisco	ASA 5500 Strong Encryption License (3DES/AES)	1
ASR1002-5G-SHA/K9	ASR1002-5G-SHA/K9	Cisco	Cisco ASR1002 Sec+HA Bundle w/ ESP-5G,AESK9,License,4GB DRAM	4
ASR1000-ESP5	ASR1000-ESP5	Cisco	Cisco ASR1K Embedded Services Processor,5Gbps,ASR1002 only	4
FLASR1-FPI-RTU	FLASR1-FPI-RTU	Cisco	Flex. Pack Insp. Right-To-Use Feat Lic,ASR1000 Series	4
FLASR1-FW-RTU	FLASR1-FW-RTU	Cisco	Firewall Right-To-Use Feature Lic for ASR1000 Series	4
FLASR1-IOSRED-RTU	FLASR1-IOSRED-RTU	Cisco	SW Redundancy Right-To-Use Feat Lic for ASR1000 Series	4
FLASR1-IPSEC-RTU	FLASR1-IPSEC-RTU	Cisco	Encryption Right-To-Use Feature Lic for ASR1000 Series	4
SASR1R1-AESK9-31S	SASR1R1-AESK9-31S	Cisco	Cisco ASR 1000 Series RP1 ADVANCED ENTERPRISE SERVICES	4
ASR1002-PWR-AC	ASR1002-PWR-AC	Cisco	Cisco ASR1002 AC Power Supply	8
CAB-AC-RA	CAB-AC-RA	Cisco	Power Cord,110V, Right Angle	8
CON-SNTP-25GSHAK9	CON-SNTP-25GSHAK 9	Cisco	SMARTNET 24X7X4 ASR1002 Sec+HA Bundle w/ESP-5G, AESK9	4
CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	4
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	4
CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	4
CIVS-IPC-2520V	CIVS-IPC-2520V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, VR	4
CON-SNT-IPC2520	CON-SNT-IPC2520	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2520V	4
IPS-4260-4GE-BP-K9	IPS-4260-4GE-BP-K9	Cisco	4260 Bundle with 4-Port Cu NIC	2

IPS-4GE-BP-INT	IPS-4GE-BP-INT	Cisco	4-Port Copper NIC with bypass for the IPS 4260 and 4270	2
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	4
CON-P2SP-4260-4G	CON-P2SP-4260-4G	Cisco	PM2, 24X7X4 IPS-4260-4GE-BP-K9	2
IPS-4260-PWR	IPS-4260-PWR	Cisco	Redundant power for 4260	2
IPS-4GE-BP-INT	IPS-4GE-BP-INT	Cisco	4-Port Copper NIC with bypass for the IPS 4260 and 4270	2
IPS-SW-6.2	IPS-SW-6.2	Cisco	Cisco IPS Sensor software version 6.2	2
WS-C3750X-24T-S	WS-C3750X-24T-S	Cisco	Cisco Catalyst 3750X 24 Port Data IP Base	8
C3KX-PWR-350WAC	C3KX-PWR-350WAC	Cisco	Cisco Catalyst 3K-X 350W AC Power Supply	8
S375XVK9T-12255SE	S375XVK9T-12255SE	Cisco	CAT 3750X IOS UNIVERSAL WITH WEB BASE DEV MGR	8
C3KX-PWR-350WAC/2	C3KX-PWR-350WAC/2	Cisco	Cisco Catalyst 3K-X 350W AC Secondary Power Supply	8
CAB-3KX-AC	CAB-3KX-AC	Cisco	AC Power Cord for Catalyst 3K-X (North America)	16
CAB-SPWR-150CM	CAB-SPWR-150CM	Cisco	3750X Stack Power Cable 150 CM - Upgrade	8
CAB-STACK-1M-NH	CAB-STACK-1M-NH	Cisco	Cisco StackWise 1M Non-Halogen Lead Free Stacking Cable	8
CON-SNTP-3750X2TS	CON-SNTP-3750X2TS	Cisco	SMARTNET 24X7X4 Catalyst 3750X 24 Port Data IP Base	8

Data Center—Service

Name	Catalog Num	Vendor	Description	Qty
ASA5585-S60-2A-K9	ASA5585-S60-2A-K9	Cisco	ASA 5585-X Chas w/ SSP60,6 GE,4 SFP+,2 GE Mgt,2 AC,3DES/AES	2
ASA-SSP-60-INC	ASA-SSP-60-INC	Cisco	ASA 5585-X Security Services Processor-60 with 6GE, 4SFP+	2
ASA-VPN-CLNT-K9	ASA-VPN-CLNT-K9	Cisco	Cisco VPN Client Software (Windows, Solaris, Linux, Mac)	2
ASA5500-ENCR-K9	ASA5500-ENCR-K9	Cisco	Cisco ASA 5500 Strong Encryption License (3DES/AES)	2
ASA5585-BLANK-F	ASA5585-BLANK-F	Cisco	Cisco ASA 5585-X Full Width Blank Slot Cover	2

ASA5585-BLANK-HD	ASA5585-BLANK-HD	Cisco	Cisco ASA 5585-X Hard Drive Blank Slot Cover	4
ASA5585-PWR-AC	ASA5585-PWR-AC	Cisco	Cisco ASA 5585-X AC Power Supply	4
ASA-ADV-END-SEC	ASA-ADV-END-SEC	Cisco	Cisco ASA 5500 Advanced Endpoint Assessment License for SSL VPN	2
ASA5500-SC-10	ASA5500-SC-10	Cisco	Cisco ASA 5500 10 Security Contexts License	2
CAB-US515P-C19-US	CAB-US515P-C19-US	Cisco	NEMA 5-15 to IEC-C19 13ft US	4
CON-SNT-A85S62K9	CON-SNT-A85S62K9	Cisco	SMARTNET 8X5XNBD ASA 5585-X Chas w/ SSP40,6 GE,4 SFP+,2 G	2
SF-ASA5585-8.2-K8	SF-ASA5585-8.2-K8	Cisco	Cisco ASA 5500 Series Software Version 8.2 for ASA 5585-X, DES	2
CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	4
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	4
CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	4
CIVS-IPC-2520V	CIVS-IPC-2520V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, VR	4
CON-SNT-IPC2520	CON-SNT-IPC2520	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2520V	4
IPS4270-2X10GE-K9	IPS4270-2X10GE-K9	Cisco	IPS 4270-20 bundled with 2-port 10GE NIC	2
IPS-2X10GE-SR-INC	IPS-2X10GE-SR-INC	Cisco	2X10GE interface card included in 10GE 4270 bundle	2
CAB-US515P-C19-US	CAB-US515P-C19-US	Cisco	NEMA 5-15 to IEC-C19 13ft US	4
CON-P2ST-IPS42702	CON-P2ST-IPS42702	Cisco	PM2, 8X5XNBD IPS 4270-20 bundled	2
IPS-2SX-INT	IPS-2SX-INT	Cisco	2-port fiber interface for the 4260 and 4270	2
IPS-4GE-BP-INT	IPS-4GE-BP-INT	Cisco	4-Port Copper NIC with bypass for the IPS 4260 and 4270	2
IPS-SW-7.0	IPS-SW-7.0	Cisco	Cisco IPS software version 7.0	2
WS-C6509-E	WS-C6509-E	Cisco	Cisco Catalyst 6500 Enhanced 9-slot chassis,15RU,no PS,no Fan Tray	1
BF-S720-64MB-RP	BF-S720-64MB-RP	Cisco	Bootflash for SUP720-64MB-RP	2
MEM-C6K-CPTFL1GB	MEM-C6K-CPTFL1GB	Cisco	Cisco Catalyst 6500 Compact Flash Memory 1GB	2
MEM-XCEF720-256M	MEM-XCEF720-256M	Cisco	Cisco Catalyst 6500 256MB DDR, xCEF720 (67xx interface, DFC3A)	1

VS-F6K-MSFC3	VS-F6K-MSFC3	Cisco	Cisco Catalyst 6500 Multilayer Switch Feature Card (MSFC) III	2
VS-F6K-PFC3C	VS-F6K-PFC3C	Cisco	Cisco Catalyst 6500 Sup 720-10G Policy Feature Card 3C	2
VS-S720-10G	VS-S720-10G	Cisco	Cisco Catalyst 6500 Supervisor 720 with 2 10GbE ports	2
WS-F6700-CFC	WS-F6700-CFC	Cisco	Cisco Catalyst 6500 Central Fwd Card for WS-X67xx modules	1
WS-F6700-DFC3CXL	WS-F6700-DFC3CXL	Cisco	Cisco Catalyst 6500 Dist Fwd Card- 3CXL, for WS-X67xx	1
WS-X6716-10GE	WS-X6716-10GE	Cisco	Cisco Catalyst 6500 16 port 10 Gigabit Ethernet Base Module	1
ACE-16G-LIC	ACE-16G-LIC	Cisco	ACE20 16Gbps License	1
ACE-SSL-05K-K9	ACE-SSL-05K-K9	Cisco	Application Control Engine SSL License, 5000 TPS	1
ACE-VIRT-020	ACE-VIRT-020	Cisco	Application Control Engine Virtualization 20 Contexts	1
ACE20-MOD-K9	ACE20-MOD-K9	Cisco	Application Control Engine 20 Hardware	1
CAB-AC-C6K-TWLK	CAB-AC-C6K-TWLK	Cisco	Power Cord, 250Vac 16A, twist lock NEMA L6-20 plug, US	4
CF-ADAPTER-SP	CF-ADAPTER-SP	Cisco	SP adapter for SUP720 and SUP720-10G	2
CON-P2OS-WIDSBNK9	CON-P2OS-WIDSBNK 9	Cisco	PM2,OS 8X5XNBD 600M IDSM-2 Mod for	1
CON-SNT-ACE20MOD	CON-SNT-ACE20MOD	Cisco	SMARTNET 8X5XNBD Application Control	1
CON-SNT-WS-FWM1K9	CON-SNT-WS-FWM1K 9	Cisco	8x5xNBD Svc, Firewall blade for Catalyst 6500	1
MEM-C6K-CPTFL1GB	MEM-C6K-CPTFL1GB	Cisco	Cisco Catalyst 6500 Compact Flash Memory 1GB	2
SC-SVC-IPSV7.0-K9	SC-SVC-IPSV7.0-K9	Cisco	IPS Software v7.0 for IDSM2	1
SC6K-A23-ACE	SC6K-A23-ACE	Cisco	ACE Module Software A2(3)	1
SV33ISK9C-12233SXI	SV33ISK9C-12233SXI	Cisco	Cisco CAT6000-VSS720 IOS IP SERVICES SSH - DEFAULT	1
VS-S720-10G-3C	VS-S720-10G-3C	Cisco	Cat 6500 Supervisor 720 with 2 ports 10GbE and MSFC3 PFC3C	2
WS-C6509-E-FAN	WS-C6509-E-FAN	Cisco	Cisco Catalyst 6509-E Chassis Fan Tray	1
WS-CAC-6000W	WS-CAC-6000W	Cisco	Cat6500 6000W AC Power Supply	2
WS-SVC-IDS2-BUN-K9	WS-SVC-IDS2-BUN-K 9	Cisco	600M IDSM-2 Mod for Cat	1

WS-X6716-10G-3CXL	WS-X6716-10G-3CXL	Cisco	Cisco Catalyst 6500 16 port 10 Gigabit Ethernet w/ DFC3CXL(req X2)	1
WS-X6748-GE-TX	WS-X6748-GE-TX	Cisco	Cat6500 48-port 10/100/1000 GE Mod: fabric enabled, RJ-45	1
X2-10GB-SR	X2-10GB-SR	Cisco	10GBASE-SR X2 Module	18
WS-C6509-E	WS-C6509-E	Cisco	Cisco Catalyst 6500 Enhanced 9-slot chassis,15RU,no PS,no Fan Tray	1
BF-S720-64MB-RP	BF-S720-64MB-RP	Cisco	Bootflash for SUP720-64MB-RP	2
MEM-C6K-CPTFL1GB	MEM-C6K-CPTFL1GB	Cisco	Cisco Catalyst 6500 Compact Flash Memory 1GB	2
MEM-XCEF720-256M	MEM-XCEF720-256M	Cisco	Cisco Catalyst 6500 256MB DDR, xCEF720 (67xx interface, DFC3A)	1
VS-F6K-MSFC3	VS-F6K-MSFC3	Cisco	Cisco Catalyst 6500 Multilayer Switch Feature Card (MSFC) III	2
VS-F6K-PFC3C	VS-F6K-PFC3C	Cisco	Cisco Catalyst 6500 Sup 720-10G Policy Feature Card 3C	2
VS-S720-10G	VS-S720-10G	Cisco	Cisco Catalyst 6500 Supervisor 720 with 2 10GbE ports	2
WS-F6700-CFC	WS-F6700-CFC	Cisco	Cisco Catalyst 6500 Central Fwd Card for WS-X67xx modules	1
WS-F6700-DFC3CXL	WS-F6700-DFC3CXL	Cisco	Cisco Catalyst 6500 Dist Fwd Card- 3CXL, for WS-X67xx	1
WS-X6716-10GE	WS-X6716-10GE	Cisco	Cisco Catalyst 6500 16 port 10 Gigabit Ethernet Base Module	1
ACE-16G-LIC	ACE-16G-LIC	Cisco	ACE20 16Gbps License	1
ACE-SSL-05K-K9	ACE-SSL-05K-K9	Cisco	Application Control Engine SSL License, 5000 TPS	1
ACE-VIRT-020	ACE-VIRT-020	Cisco	Application Control Engine Virtualization 20 Contexts	1
ACE20-MOD-K9	ACE20-MOD-K9	Cisco	Application Control Engine 20 Hardware	1
CAB-AC-C6K-TWLK	CAB-AC-C6K-TWLK	Cisco	Power Cord, 250Vac 16A, twist lock NEMA L6-20 plug, US	4
CF-ADAPTER-SP	CF-ADAPTER-SP	Cisco	SP adapter for SUP720 and SUP720-10G	2
CON-P2OS-WIDSBNK9	CON-P2OS-WIDSBNK 9	Cisco	PM2,OS 8X5XNBD 600M IDSM-2 Mod for	1
CON-SNT-ACE20MOD	CON-SNT-ACE20MOD	Cisco	SMARTNET 8X5XNBD Application Control	1
CON-SNT-WS-FWM1K9	CON-SNT-WS-FWM1K 9	Cisco	8x5xNBD Svc, Firewall blade for Catalyst 6500	1
MEM-C6K-CPTFL1GB	MEM-C6K-CPTFL1GB	Cisco	Cisco Catalyst 6500 Compact Flash Memory 1GB	2

SC-SVC-IPSV7.0-K9	SC-SVC-IPSV7.0-K9	Cisco	IPS Software v7.0 for IDSM2	1
SC6K-A23-ACE	SC6K-A23-ACE	Cisco	ACE Module Software A2(3)	1
SV33ISK9C-12233SXI	SV33ISK9C-12233SXI	Cisco	Cisco CAT6000-VSS720 IOS IP SERVICES SSH - DEFAULT	1
VS-S720-10G-3C	VS-S720-10G-3C	Cisco	Cat 6500 Supervisor 720 with 2 ports 10GbE and MSFC3 PFC3C	2
WS-C6509-E-FAN	WS-C6509-E-FAN	Cisco	Cisco Catalyst 6509-E Chassis Fan Tray	1
WS-CAC-6000W	WS-CAC-6000W	Cisco	Cat6500 6000W AC Power Supply	2
WS-SVC-IDS2-BUN-K9	WS-SVC-IDS2-BUN-K 9	Cisco	600M IDSM-2 Mod for Cat	1
WS-X6716-10G-3CXL	WS-X6716-10G-3CXL	Cisco	Cisco Catalyst 6500 16 port 10 Gigabit Ethernet w/ DFC3CXL(req X2)	1
WS-X6748-GE-TX	WS-X6748-GE-TX	Cisco	Cat6500 48-port 10/100/1000 GE Mod: fabric enabled, RJ-45	1
X2-10GB-SR	X2-10GB-SR	Cisco	10GBASE-SR X2 Module	18

Data Center—Secure Storage

Name	Catalog Num	Vendor	Description	Qty
DS-C9509-2AK9	DS-C9509-2AK9	Cisco	MDS 9509 Base Config: Chassis, 2 Sup-2A, 2 3K AC PS	2
CAB-9K16A-US2	CAB-9K16A-US2	Cisco	Power Cord 250VAC 16A, US/Japan, Src Plug NEMA L6-20	4
CON-SNT-4848K	CON-SNT-4848K	Cisco	SMARTNET 8X5XNBD Host Optimized 8G FC	4
CON-SNT-9304K	CON-SNT-9304K	Cisco	SMARTNET 8X5XNBD MDS 9000 18-port FC and 4-port GE Module	2
CON-SNT-C9509U	CON-SNT-C9509U	Cisco	SMARTNET 8X5XNBD MDS 9509 Base Config: Chassis, 2 Sup-2A	2
DS-9509-KIT-EMC	DS-9509-KIT-EMC	Cisco	MDS 9509 Accessory Kit for EMC	2
DS-SFP-FC4G-SW	DS-SFP-FC4G-SW	Cisco	4 Gbps Fibre Channel-SW SFP, LC	36
DS-SFP-FC8G-SW	DS-SFP-FC8G-SW	Cisco	8 Gbps Fibre Channel SW SFP+, LC	192
DS-X9248-48K9	DS-X9248-48K9	Cisco	4/44-Port Host-Optimized 8-Gbps FC Module	4
DS-X9304-18K9	DS-X9304-18K9	Cisco	MDS 9000 18-port FC and 4-port GE Module	2

M9500ENT1K9	M9500ENT1K9	Cisco	Enterprise package license for 1 MDS9500 switch	2
M9500SSE1K9	M9500SSE1K9	Cisco	Storage Services Enabler: 1 ASM on 1 MDS9500	2
M95IOA184	M95IOA184	Cisco	Cisco I/O Accelerator License for MSM-18/4 on MDS 9500	2
M95S2K9-5.0.4	M95S2K9-5.0.4	Cisco	MDS 9500 Supervisor/Fabric-2, NX-OS Software Release 5.0(4)	2
SSI-M9K9-504	SSI-M9K9-504	Cisco	MDS SSI Image 5.0(4)	2

Data Center—Extranet Edge

Name	Catalog Num	Vendor	Description	Qty
ASA5555-IPS-K9	ASA5555-IPS-K9	Cisco	ASA 5555-X with IPS, SW, 8GE Data, 1GE Mgmt, AC, 3DES/AES	1
ASA5500-SSL-10	ASA5500-SSL-10	Cisco	ASA 5500 SSL VPN 10 Premium User License	1
ASA-ADV-END-SEC	ASA-ADV-END-SEC	Cisco	ASA 5500 Advanced Endpoint Assessment License for SSL VPN	1
ASA-AC-E-5555	ASA-AC-E-5555	Cisco	AnyConnect Essentials VPN License - ASA 5555-X (5000 Users)	1
ASA-VPNP-5555	ASA-VPNP-5555	Cisco	Premium Shared VPN Participant License - ASA 5555-X	1
ASA-AC-M-5555	ASA-AC-M-5555	Cisco	AnyConnect Mobile - ASA 5555-X (req. Essentials or Premium)	1
ASA5500-SC-5	ASA5500-SC-5	Cisco	ASA 5500 5 Security Contexts License	1
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	1
SF-ASA-9.1-K8	SF-ASA-9.1-K8	Cisco	ASA 5500 Series Software Ver. 9.1 for ASA 5512X--5555X, DES	1
SF-ASAIPS64-7.1-K9	SF-ASAIPS64-7.1-K9	Cisco	ASA 5500-X IPS Software 7.1 for IPS SSP	1
ASA5555-IPS-SSP	ASA5555-IPS-SSP	Cisco	ASA 5555-X IPS SSP License	1
ASA-PWR-AC	ASA-PWR-AC	Cisco	ASA 5545-X/5555-X AC Power Supply	1
ASA-PWR-BLANK	ASA-PWR-BLANK	Cisco	ASA 5545-X/5555-X Power Slot Blank Cover	1
ASA5500-ENCR-K9	ASA5500-ENCR-K9	Cisco	ASA 5500 Strong Encryption License (3DES/AES)	1

ASR1002-5G-SHA/K9	ASR1002-5G-SHA/K9	Cisco	Cisco ASR1002 Sec+HA Bundle w/ ESP-5G,AESK9,License,4GB DRAM	2
ASR1000-ESP5	ASR1000-ESP5	Cisco	Cisco ASR1K Embedded Services Processor,5Gbps,ASR1002 only	2
FLASR1-FPI-RTU	FLASR1-FPI-RTU	Cisco	Flex. Pack Insp. Right-To-Use Feat Lic,ASR1000 Series	2
FLASR1-FW-RTU	FLASR1-FW-RTU	Cisco	Firewall Right-To-Use Feature Lic for ASR1000 Series	2
FLASR1-IOSRED-RTU	FLASR1-IOSRED-RTU	Cisco	SW Redundancy Right-To-Use Feat Lic for ASR1000 Series	2
FLASR1-IPSEC-RTU	FLASR1-IPSEC-RTU	Cisco	Encryption Right-To-Use Feature Lic for ASR1000 Series	2
SASR1R1-AESK9-31S	SASR1R1-AESK9-31S	Cisco	Cisco ASR 1000 Series RP1 ADVANCED ENTERPRISE SERVICES	2
ASR1002-PWR-AC	ASR1002-PWR-AC	Cisco	Cisco ASR1002 AC Power Supply	4
CAB-AC-RA	CAB-AC-RA	Cisco	Power Cord,110V, Right Angle	4
CON-SNTP-25GSHAK9	CON-SNTP-25GSHAK 9	Cisco	SMARTNET 24X7X4 ASR1002 Sec+HA Bundle w/ESP-5G, AESK9	2
ASR1004-20G-HA/K9	ASR1004-20G-HA/K9	Cisco	ASR1004 HA Bundle w/ ESP-20G,RP1,SIP10,AESK9,License	2
ASR1000-ESP20	ASR1000-ESP20	Cisco	Cisco ASR1000 Embedded Services Processor, 20G	2
ASR1000-SPA	ASR1000-SPA	Cisco	SPA for ASR1000; No Physical Part; For Tracking Only	4
FLASR1-IOSRED-RTU	FLASR1-IOSRED-RTU	Cisco	SW Redundancy Right-To-Use Feat Lic for ASR1000 Series	2
M-ASR1K-HDD-40GB	M-ASR1K-HDD-40GB	Cisco	Cisco ASR1000 RP1 40GB HDD	2
M-ASR1K-RP1-4GB	M-ASR1K-RP1-4GB	Cisco	Cisco ASR1000 RP1 4GB DRAM	2
SASR1R1-AESK9-31S	SASR1R1-AESK9-31S	Cisco	Cisco ASR 1000 Series RP1 ADVANCED ENTERPRISE SERVICES	2
ASR1000-RP1-BUN	ASR1000-RP1-BUN	Cisco	Cisco ASR1000 Route Processor 1, 4GB DRAM,Bundle Component	2
ASR1000-SIP10	ASR1000-SIP10	Cisco	Cisco ASR1000 SPA Interface Processor 10	2
ASR1000-SIP10-BUN	ASR1000-SIP10-BUN	Cisco	Cisco ASR1000 SPA Interface Processor 10, Bundle Component	2
ASR1004-PWR-AC	ASR1004-PWR-AC	Cisco	Cisco ASR1004 AC Power Supply	4
CAB-AC15A-90L-US	CAB-AC15A-90L-US	Cisco	15A AC Pwr Cord, left-angle (United States) (bundle option)	4
CON-SNTP-420GHAK9	CON-SNTP-420GHAK 9	Cisco	SMARTNET 24X7X4 ASR1004 Chassis 2 P/S	2

CON-SNTP-A1ESP20	CON-SNTP-A1ESP20	Cisco	SMARTNET 24X7X4 ASR1000 Embedded Svc Processor,20G,Crypt	2
CON-SNTP-ASRRP1B	CON-SNTP-ASRRP1B	Cisco	SMARTNET 24X7X4 Cisco ASR1000 Route Processor 1	2
CON-SNTP-ASRSIPB	CON-SNTP-ASRSIPB	Cisco	SMARTNET 24X7X4 Cisco ASR1000 SPA Interface Processor	2
FLASR1-FW-RTU	FLASR1-FW-RTU	Cisco	Firewall Right-To-Use Feature Lic for ASR1000 Series	2
SPA-1X10GE-L-V2	SPA-1X10GE-L-V2	Cisco	Cisco 1-Port 10GE LAN-PHY Shared Port Adapter	4
XFP-10G-MM-SR	XFP-10G-MM-SR	Cisco	10GBASE-SR XFP Module	4
CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	4
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	4
CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	4
CIVS-IPC-2520V	CIVS-IPC-2520V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, VR	4
CON-SNT-IPC2520	CON-SNT-IPC2520	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2520V	4
IPS-4260-4GE-BP-K9	IPS-4260-4GE-BP-K9	Cisco	4260 Bundle with 4-Port Cu NIC	2
IPS-4GE-BP-INT	IPS-4GE-BP-INT	Cisco	4-Port Copper NIC with bypass for the IPS 4260 and 4270	2
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	4
CON-P2SP-4260-4G	CON-P2SP-4260-4G	Cisco	PM2, 24X7X4 IPS-4260-4GE-BP-K9	2
IPS-4260-PWR	IPS-4260-PWR	Cisco	Redundant power for 4260	2
IPS-4GE-BP-INT	IPS-4GE-BP-INT	Cisco	4-Port Copper NIC with bypass for the IPS 4260 and 4270	2
IPS-SW-6.2	IPS-SW-6.2	Cisco	Cisco IPS Sensor software version 6.2	2
N5K-C5020P-NBF	N5K-C5020P-NBF	Cisco	Cisco Nexus 5020 NetApp OSM version, 2 PS	2
N5020-ACC-KIT	N5020-ACC-KIT	Cisco	Nexus 5020 Accessory Kit, Option	2
N5K-PAC-1200W	N5K-PAC-1200W	Cisco	Nexus 5020 PSU module, 100-240VAC 1200W	4
CAB-9K12A-NA	CAB-9K12A-NA	Cisco	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	4
CON-SNTP-N5020	CON-SNTP-N5020	Cisco	SMARTNET 24X7X4 N5000 2RU Chassis no PS 5	2

N5000FMS1K9	N5000FMS1K9	Cisco	Nexus 5000 Fabric Manager Server License	2
N5K-M1600	N5K-M1600	Cisco	N5000 1000 Series Module 6port 10GE(req SFP+)	4
N5KUK9-421N2.1	N5KUK9-421N2.1	Cisco	Nexus 5000 Base OS Software Rel 4.2(1)N2(1)	2
SFP-H10GB-CU1M	SFP-H10GB-CU1M	Cisco	10GBASE-CU SFP+ Cable 1 Meter	16
SFP-H10GB-CU3M	SFP-H10GB-CU3M	Cisco	10GBASE-CU SFP+ Cable 3 Meter	64
WS-C3750X-24T-S	WS-C3750X-24T-S	Cisco	Cisco Catalyst 3750X 24 Port Data IP Base	8
C3KX-PWR-350WAC	C3KX-PWR-350WAC	Cisco	Cisco Catalyst 3K-X 350W AC Power Supply	8
S375XVK9T-12255SE	S375XVK9T-12255SE	Cisco	CAT 3750X IOS UNIVERSAL WITH WEB BASE DEV MGR	8
C3KX-PWR-350WAC/2	C3KX-PWR-350WAC/2	Cisco	Cisco Catalyst 3K-X 350W AC Secondary Power Supply	8
CAB-3KX-AC	CAB-3KX-AC	Cisco	AC Power Cord for Catalyst 3K-X (North America)	16
CAB-SPWR-150CM	CAB-SPWR-150CM	Cisco	3750X Stack Power Cable 150 CM - Upgrade	8
CAB-STACK-1M-NH	CAB-STACK-1M-NH	Cisco	Cisco StackWise 1M Non-Halogen Lead Free Stacking Cable	8
CON-SNTP-3750X2TS	CON-SNTP-3750X2TS	Cisco	SMARTNET 24X7X4 Catalyst 3750X 24 Port Data IP Base	8

Data Center—Physical Security

Name	Catalog Num	Vendor	Description	Qty
CIAC-GW-K9	CIAC-GW-K9	Cisco	Cisco Physical Access Gateway	8
CIAC-GW-SW-1.0-K9	CIAC-GW-SW-1.0-K9	Cisco	Cisco Physical Access Gateway Software Version 1.0	8
CON-SNT-GWK9	CON-SNT-GWK9	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	8
CIAC-PAME-1125-K9	CIAC-PAME-1125-K9	Cisco	Cisco Physical Access Manager Appliance	4
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	4
CIAC-SW-LNX-1.0-K9	CIAC-SW-LNX-1.0-K9	Cisco	Cisco PAM Appliance Software Version 1.0	4
CON-SNT-PAM1125	CON-SNT-PAM1125	Cisco	SMARTNET 8X5XNBD Cisco Physical Access	4

CIVS-IPC-2421	CIVS-IPC-2421	Cisco	Cisco Indoor SD IP Dome, 2.8-10mm, D/N, Smoked, CM	4
CON-SNT-IPC2421	CON-SNT-IPC2421	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2421	4
CIVS-IPC-2500	CIVS-IPC-2500	Cisco	Cisco 2500 IP Camera, Full Resolution, Day/Night	4
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	4
CIVS-IPC-VT55	CIVS-IPC-VT55	Cisco	Cisco IP Camera Tamron 5-50mm Varifocal Lens	4
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	4
CON-SNT-IPC2500	CON-SNT-IPC2500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2500	4
CIVS-IPC-2520V	CIVS-IPC-2520V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, VR	4
CON-SNT-IPC2520	CON-SNT-IPC2520	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2520V	4
CIVS-IPC-2521V	CIVS-IPC-2521V	Cisco	Cisco SD IP Dome, 2.8-10mm, D/N, Smoked, VR	4
CON-SNT-IPC2521	CON-SNT-IPC2521	Cisco	SMARTNET 8X5XNBD CIVS-IPC-2521V	4
CIVS-IPC-4500	CIVS-IPC-4500	Cisco	Cisco 4500 IP Camera, HD, DSP, Day/Night	4
CIVS-CAB-BAC	CIVS-CAB-BAC	Cisco	CIVS C15 Power Cable North America	4
CIVS-IPC-VFM15-50	CIVS-IPC-VFM15-50	Cisco	Cisco IP Camera Lens Megapixel 15-50mm Fujinon	4
CIVS-PWRPAC-12V	CIVS-PWRPAC-12V	Cisco	Cisco VS External Dual Voltage Power Supply for Encode/Dec	4
CON-SNT-IPC4500	CON-SNT-IPC4500	Cisco	SMARTNET 8X5XNBD CIVS-IPC-4500	4
CIVS-IPC-5010	CIVS-IPC-5010	Cisco	Cisco Video Surveillance IP Camera, Indoor HD Dome (Clear)	4
CON-SNT-CIVSIPC1	CON-SNT-CIVSIPC1	Cisco	SMARTNET 8X5XNBD Cisco Video Surveillance IP Camera	4
CIVS-IPC-5011	CIVS-IPC-5011	Cisco	Cisco Video Surveillance IP Camera, Indoor HD Dome (Smoked)	4
CON-SNT-CIVSIPC0	CON-SNT-CIVSIPC0	Cisco	SMARTNET 8X5XNBD Cisco Video Surveillance IP Camera, Indo	4
CIVS-MSP-4RU	CIVS-MSP-4RU	Cisco	4RU w/Motherboard;1 CPU;RAID;Pwr Suppl;NO Drives;NO Options	2
CIVS-CAB-16-AC	CIVS-CAB-16-AC	Cisco	CIVS C16 Power Cable North America	4
CIVS-FC-1P	CIVS-FC-1P	Cisco	1 Port FibreChannel Card for CIVS-MSP	2

CIVS-HDD-1000	CIVS-HDD-1000	Cisco	1TB SATA Drive for CIVS-MSP	48
CIVS-MS-SW6.2	CIVS-MS-SW6.2	Cisco	CIVS-MS Media Server v6.2 Software License with Hardware	2
CIVS-PS-900	CIVS-PS-900	Cisco	Redundant 900W Power Supply for CIVS-MSP 2RU, 4RU	2
CIVS-VSM-SW4262	CIVS-VSM-SW4262	Cisco	CIVS-VSM Video Surveillance Manager v4.2/6.2 SW Mfg Image	2
CON-SNT-VSM4U	CON-SNT-VSM4U	Cisco	SMARTNET 8X5XNBD 4RU MSP Assembly	2
CIVS-SS-4U-42000	CIVS-SS-4U-42000	Cisco	Cisco VS 4U Storage System with 42x1000GB drives	4
CON-SNT-VSS442K	CON-SNT-VSS442K	Cisco	SMARTNET 8X5XNBD CIVS-SS-4U-42000	4
CIVS-VM-1DFL=	CIVS-VM-1DFL=	Cisco	Cisco VS Virtual Matrix Client License, 1 client	10
CIVS-VM-SW6.2=	CIVS-VM-SW6.2=	Cisco	CIVS-VM Virtual Matrix v6.2 Software License	1
CON-SAS-VMSW62	CON-SAS-VMSW62	Cisco	SW APP SUPP CIVS-VM Virtual Matrix v6.2 Software Lic	1

Data Center—Wireless Systems

Name	Catalog Num	Vendor	Description	Qty
AIR-CT5508-500-2PK	AIR-CT5508-500-2PK	Cisco	2x AIR-CT5508-500-K9	2
AIR-PWR-CORD-NA	AIR-PWR-CORD-NA	Cisco	AIR Line Cord North America	4
LIC-CT5508-500	LIC-CT5508-500	Cisco	500 AP Base license	4
LIC-CT5508-BASE	LIC-CT5508-BASE	Cisco	Base Software License	4
SWC5500K9-70	SWC5500K9-70	Cisco	Cisco Unified Wireless Controller SW Release 7.0	4
AIR-CT5508-500-K9Z	AIR-CT5508-500-K9Z	Cisco	5508 Series Controller for up to 500 APs	4
CON-SNTP-AIRC552P	CON-SNTP-AIRC552P	Cisco	SMARTNET 24X7X4 Two 5508 Series Controller for up to 500	2
AIR-MSE-3355-K9	AIR-MSE-3355-K9	Cisco	MSE 3355 Hardware SKU	2
AIR-MSE-PAK	AIR-MSE-PAK	Cisco	Mobility Services Configurable PAK	2
AIR-PWR-CORD-NA	AIR-PWR-CORD-NA	Cisco	AIR Line Cord North America	2

AIR-WIPS-AP-2000	AIR-WIPS-AP-2000	Cisco	Cisco wIPS License, Supporting Cisco 2000 Monitor Mode APs	2
SWMSE3355K9-70	SWMSE3355K9-70	Cisco	Cisco 3355 Series Mobility Services Engine SW Release 7.0	2
WCS-CD-K9	WCS-CD-K9	Cisco	CD With Windows And Linux. No License.	4
WCS-ENT-PLUS-K9	WCS-ENT-PLUS-K9	Cisco	Family SKU for WCS Enterprise PLUS License Products	1
CON-SAU-WENTK9	CON-SAU-WENTK9	Cisco	SW APP SUPP + UPGR Family SKU for WCS E	1
WCS-ENT-PLUS-10000	WCS-ENT-PLUS-10000	Cisco	Cisco WCS Enterprise PLUS License for 10,000 APs, Win/Linux	1

Data Center—Management

Note Previous validation included ACS 4.2.1 on Windows as shown in the implementation section 5. Subsequent validation was achieved for the Cisco ACS 5.3 appliance and is the recommended product in this BOM.

Name	Catalog Num	Vendor	Description	Qty
CSACS-1121-K9	CSACS-1121-K9	Cisco	ACS 1121 Appliance With 5.x SW And Base license	2
CSACS-5-BASE-LIC	CSACS-5-BASE-LIC	Cisco	Cisco Secure ACS 5 Base License	2
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	2
CON-SNTP-SACS1121	CON-SNTP-SACS1121	Cisco	SMARTNET 24X7X4 ACS 1121 Appliance With 5.1	2
CSACS-5-ADV-LIC	CSACS-5-ADV-LIC	Cisco	ACS 5 Security Group Access System License	2
CSACS-5.2-SW-K9	CSACS-5.2-SW-K9	Cisco	Config Option: ACS 5.2 Software Loaded On 1121	2
CSMPR-LIC-1000	CSMPR-LIC-1000	Cisco	Cisco Security Manager Pro - Incremental 1000 Device License	1
CON-P2S-CSMPRI1K	CON-P2S-CSMPRI1K	Cisco	PM2, SAS CSM Ent Pro -1K incr. dev license	1
CSMPR50-4.0-K9	CSMPR50-4.0-K9	Cisco	Cisco Security Manager 4.0 Professional w/ 50 Device License	1
CSMPR50-PAK4	CSMPR50-PAK4	Cisco	CS Mgr Enterprise Pro 50 - Secondary PAK	1
CON-CSSPS-CSMPR504	CON-CSSPS-CSMPR504	Cisco	SHARED SUPP SAS CS Mgr 4.0 Enterprise Pro 50 DeviceBase	1

CSMPR50-U-4.0-K9	CSMPR50-U-4.0-K9	Cisco	Cisco Security Manager 3.x to 4.0 Upgrade - PRO-50 License	1
CSMPR50-PAK4	CSMPR50-PAK4	Cisco	CS Mgr Enterprise Pro 50 - Secondary PAK	1
NAC3355-3500-K9	NAC3355-3500-K9	Cisco	NAC Appliance 3355 Server -max 3500 users	4
NAC3355-95-CAVACC	NAC3355-95-CAVACC	Cisco	NAC Appliance 3355-95 Cavium Accelerator	4
NAC3355-SVR	NAC3355-SVR	Cisco	NAC Appliance 3355 Server Hardware	4
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	8
CON-SNT-NAC535M	CON-SNT-NAC535M	Cisco	SMARTNET 8X5XNBD NAC3355-3500-K9	4
NAC-SVR-48-K9	NAC-SVR-48-K9	Cisco	NAC Appliance Server Release 4.8	4
NACMGR-M-STD-K9	NACMGR-M-STD-K9	Cisco	Cisco NAC Standard Manager for 20 servers	2
NAC3355	NAC3355	Cisco	NAC Appliance 3355 Manager Hardware	2
NAC3355-95-CAVACC	NAC3355-95-CAVACC	Cisco	NAC Appliance 3355-95 Cavium Accelerator	2
CAB-AC	CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	4
CON-SNT-NAMSTDK9	CON-SNT-NAMSTDK9	Cisco	SMARTNET 8X5XNBD NACMGR-M-STD-K9	2
SPESMA-VC-BASE	SPESMA-VC-BASE	Cisco	EMC VoyenceControl Base	1
SP-PRODUCTS-TERMS	SP-PRODUCTS-TERMS	Cisco	Buyer Acceptance of SolutionsPlus Terms and Conditions	1
SPESMA-VC-LIC	SPESMA-VC-LIC	Cisco	EMC VoyenceControl License Card	1
SPESMA-VCMD-P	SPESMA-VCMD-P	Cisco	EMC VoyenceControl Prod Lic (RTU Lic per NOC/Data Ctr)	1
SPESMA-VCMD1-03	SPESMA-VCMD1-03	Cisco	EMC VoyenceControl Managed Tier 1 Device License: 1001-1500	1,200
SPESMA-VCMD2-03	SPESMA-VCMD2-03	Cisco	EMC VoyenceControl Managed Tier 2 Device License: 1001-1500	1,200
SPESMA-VCMD3-03	SPESMA-VCMD3-03	Cisco	EMC VoyenceControl Managed Tier 3 Device License: 1001-1500	1,200
SPESMA-VCO-LIC	SPESMA-VCO-LIC	Cisco	EMC Voyence PCI Advisor License Card	1
SPESMA-VCO-NA02	SPESMA-VCO-NA02	Cisco	EMC Voyence Network Advisor - Less Than 10,000 Devices	1
SPESMA-VCO-PCI	SPESMA-VCO-PCI	Cisco	EMC Voyence PCI Advisor	1

Data Center—Access, Aggregation

Name	Catalog Num	Vendor	Description	Qty
L-VLVSG-VNMC=	L-VLVSG-VNMC=	Cisco	Virtual Network Mgmt Center Base License for VSG eDelivery	1
CON-CSSPU-LVLVSG	CON-CSSPU-LVLVSG	Cisco	SHARED SUPP SAU Virtual Network Mgmt Center Base for VSG	1
CON-SAU-LVLVSG	CON-SAU-LVLVSG	Cisco	SW APP SUPP + UPGR Virtual Network Mgmt Center Base for VSG	1
L-VLVSG-VNMC-P1	L-VLVSG-VNMC-P1	Cisco	VSG and VNMC eDelivery CPU License Promo 1 Qty 32	32
N1K-C1010	N1K-C1010	Cisco	Cisco Nexus 1010 Virtual Services Appliance	1
A01-X0105	A01-X0105	Cisco	2.66GHz Xeon X5650 95W CPU/12MB cache/DDR3 1333MHz	2
CAB-C13-C14-JMPR	CAB-C13-C14-JMPR	Cisco	Recessed receptical AC power cord 27	1
N01-M304GB1	N01-M304GB1	Cisco	4GB DDR3-1333MHz RDIMM/PC3-10600/dual rank 1Gb DRAMs	4
N1K-VLCPU-32	N1K-VLCPU-32	Cisco	Nexus 1000V for Nexus 1010 Paper CPU License Qty 32	1
N2XX-ABPCI03	N2XX-ABPCI03	Cisco	Broadcom 5709 Quad Port 10/100/1Gb NIC w/TOE iSCSI	1
R200-BBLKD	R200-BBLKD	Cisco	HDD slot blanking panel for UCS C200 M1 Rack Servers	2
R200-BHTS1	R200-BHTS1	Cisco	CPU heat sink for UCS C200 M1 Rack Server	2
R200-D500GCSATA03	R200-D500GCSATA03	Cisco	Gen 2 500GB SATA 7.2K RPM 3.5in HDD/hot plug/C200 drive sled	2
R200-PCIBLKF1	R200-PCIBLKF1	Cisco	PCIe Full Height blanking panel for UCS C-Series Rack Server	1
R200-SASCBL-001	R200-SASCBL-001	Cisco	Internal SAS Cable for a base UCS C200 M1 Server	1
R2X0-ML002	R2X0-ML002	Cisco	LSI 1064E (4-port SAS 3.0G RAID 0, 1, 1E) Mezz Card	1
R2X0-PSU2-650W-SB	R2X0-PSU2-650W-SB	Cisco	650W power supply, w/added 5A Standby for UCS C200 or C210	1
R2XX-CMAG3-1032	R2XX-CMAG3-1032	Cisco	Cable Mgmt Arm for R2XX-G31032RAIL for C200/C210	1
R2XX-G31032RAIL	R2XX-G31032RAIL	Cisco	G3 shorter stronger Rail Kit for UCS 200, 210 Rack Servers	1
R2XX-PSUBLKP	R2XX-PSUBLKP	Cisco	Power supply unit blnking pnl for UCS 200 M1 or 210 M1	1

R2XX-RAID1	R2XX-RAID1	Cisco	Enable RAID 1 Setting	1
CAB-N5K6A-NA	CAB-N5K6A-NA	Cisco	Power Cord, 200/240V 6A North America	1
N1K-VLCPU-32=	N1K-VLCPU-32=	Cisco	Nexus 1000V Paper CPU License Qty 32 (1YR Min Service)	1
N1K-VLCPU-01	N1K-VLCPU-01	Cisco	Nexus 1000V Paper CPU License Qty 1	32
N5K-C5020P-NBF	N5K-C5020P-NBF	Cisco	Nexus 5020 NetApp OSM version, 2 PS	2
N5020-ACC-KIT	N5020-ACC-KIT	Cisco	Nexus 5020 Accessory Kit, Option	2
N5K-PAC-1200W	N5K-PAC-1200W	Cisco	Nexus 5020 PSU module, 100-240VAC 1200W	4
CAB-9K12A-NA	CAB-9K12A-NA	Cisco	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	4
CON-SNTP-N5020	CON-SNTP-N5020	Cisco	SMARTNET 24X7X4 N5000 2RU Chassis no PS 5	2
N5000FMS1K9	N5000FMS1K9	Cisco	Nexus 5000 Fabric Manager Server License	2
N5K-M1600	N5K-M1600	Cisco	N5000 1000 Series Module 6port 10GE(req SFP+)	4
N5KUK9-421N2.1	N5KUK9-421N2.1	Cisco	Nexus 5000 Base OS Software Rel 4.2(1)N2(1)	2
SFP-H10GB-CU1M	SFP-H10GB-CU1M	Cisco	10GBASE-CU SFP+ Cable 1 Meter	16
SFP-H10GB-CU3M	SFP-H10GB-CU3M	Cisco	10GBASE-CU SFP+ Cable 3 Meter	64
N7K-C7010-BUN-R	N7K-C7010-BUN-R	Cisco	Nexus 7010 Bundle (Chassis,(2)SUP1,(3)FAB1,(3)AC-6KW PSU)	2
N7K-AC-6.0KW	N7K-AC-6.0KW	Cisco	Nexus 7000 - 6.0KW AC Power Supply Module	6
N7K-C7010-FAB1-BUN	N7K-C7010-FAB1-BUN	Cisco	Nexus 7000 - 10 Slot Chassis - 46Gbps/Slot Fabric Module	6
N7K-SUP1-BUN	N7K-SUP1-BUN	Cisco	Nexus 7000 - Supervisor 1, Includes External 8GB Flash	4
CAB-AC-2500W-US1	CAB-AC-2500W-US1	Cisco	Power Cord, 250Vac 16A, straight blade NEMA 6-20 plug, US	12
CON-SNTP-C701BR	CON-SNTP-C701BR	Cisco	SMARTNET 24X7X4 Nexus 7010 Bundle	2
N7K-CPF-2GB	N7K-CPF-2GB	Cisco	Nexus Compact Flash Memory 2GB (Expansion Flash - Slot 0)	4
N7K-M132XP-12	N7K-M132XP-12	Cisco	Nexus 7000 - 32 Port 10GbE, 80G Fabric (req. SFP+)	6
N7K-M148GT-11	N7K-M148GT-11	Cisco	Nexus 7000 - 48 Port 10/100/1000, RJ-45	2

N7KS1K9-50	N7KS1K9-50	Cisco	Cisco NX-OS Release 5.0	2
SFP-10G-SR	SFP-10G-SR	Cisco	10GBASE-SR SFP Module	34
WS-C4948-10GE-S	WS-C4948-10GE-S	Cisco	Catalyst 4948, IPB s/w, 48*10/100/1000+2*10GE(X2), 1 AC p/s	2
PWR-C49-300AC	PWR-C49-300AC	Cisco	Catalyst 4948 300-Watt AC Power Supply	2
S49IPB-12253SG	S49IPB-12253SG	Cisco	Cisco CAT4900 IOS IP BASE W/O CRYPTO	2
CAB-US515-C15-US	CAB-US515-C15-US	Cisco	NEMA 5-15 to IEC-C15 8ft US	2
CON-SNT-C4948GES	CON-SNT-C4948GES	Cisco	SMARTNET 8X5XNBD 4948, IPB s/w 4810/100/1K 2 10GE	2
X2-10GB-SR=	X2-10GB-SR=	Cisco	10GBASE-SR X2 Module	4

Data Center—UCS

Name	Catalog Num	Vendor	Description	Qty
N20-Z0001	N20-Z0001	Cisco	Cisco Unified Computing System	1
N1K-VLEM-UCS-1	N1K-VLEM-UCS-1	Cisco	Nexus 1000V License PAK For 1 Virtual Ethernet Module On UCS	32
VMW-VS-ENTP-1A	VMW-VS-ENTP-1A	Cisco	VMware vSphere Enterprise Plus (1 CPU), 1yr support required	32
A01-X0100	A01-X0100	Cisco	3.33GHz Xeon X5680 130W CPU/12MB cache/DDR3 1333MHz	64
A03-D146GC2	A03-D146GC2	Cisco	146GB 6Gb SAS 15K RPM SFF HDD/hot plug/drive sled mounted	64
CAB-AC-C6K-TWLK	CAB-AC-C6K-TWLK	Cisco	Power Cord, 250Vac 16A, twist lock NEMA L6-20 plug, US	16
CAB-N5K6A-NA	CAB-N5K6A-NA	Cisco	Power Cord, 200/240V 6A North America	4
CON-ISV1-VCS1A	CON-ISV1-VCS1A	Cisco	ISV 24X7 VMware vCenter Server Std 1 Yr RQD	32
CON-ISV1-VLEMUCS	CON-ISV1-VLEMUCS	Cisco	ISV 24X7 Nexus 1000V License PAK For 1 Virtual Et	64
CON-ISV1-VSENTP1A	CON-ISV1-VSENTP1A	Cisco	ISV 24X7 VMware vSphere EntPlus1CPU 1Yr RQD	32
CON-ISV1-VSENTP3A	CON-ISV1-VSENTP3A	Cisco	ISV 24X7 VMware vSphere EntPlus1CPU 3Yr RQD	32

CON-UCS1-1E0440	CON-UCS1-1E0440	Cisco	UC SUPPORT 8X5XNBD 4PT 10GE/4PT 4Gb FC/ExpanMod 6100Series	2
CON-UCS1-1S6200	CON-UCS1-1S6200	Cisco	UC SUPPORT 8X5XNBD 6140XP 40PT Fabric Interconnect	2
CON-UCS1-2C6508	CON-UCS1-2C6508	Cisco	UC SUPPORT 8X5XNBD 5108 Blade Server Chassis	4
CON-UCS1-2Z0001	CON-UCS1-2Z0001	Cisco	UC SUPPORT 8X5XNBD Cisco Unified Computing System	1
CON-UCS1-B66251	CON-UCS1-B66251	Cisco	UC SUPPORT 8X5XNBD UCSB200 M2 Blade Svr w/o CPU Mem HDD Mez	32
DS-SFP-FC4G-SW	DS-SFP-FC4G-SW	Cisco	4 Gbps Fibre Channel-SW SFP, LC	32
N01-M308GB2-L	N01-M308GB2-L	Cisco	8GB DDR3-1333MHz RDIMM/PC3-10600/dual rank/Low Voltage	384
N01-UAC1	N01-UAC1	Cisco	Single phase AC power module for UCS 5108	4
N10-E0440	N10-E0440	Cisco	4-port 10 GE/4-port 4Gb FC/Expansion module/UCS 6100 Series	2
N10-L001	N10-L001	Cisco	UCS 6100 Series Fabric Interconnect 1 10GE port license	32
N10-MGT005	N10-MGT005	Cisco	UCS Manager v1.3	2
N10-PAC2-750W	N10-PAC2-750W	Cisco	750W power supply unit for UCS 6140XP/100-240VAC	4
N10-S6200	N10-S6200	Cisco	UCS 6140XP 40-port Fabric Interconnect/0 PSU/5 fans/no SFP+	2
N10-SACCB	N10-SACCB	Cisco	Accessory kit for UCS 6140XP Fabric Interconnect	2
N10-SBLKE	N10-SBLKE	Cisco	Expansion module slot blanking panel for UCS 6100 Series	2
N1K-CSK9-UCS-404	N1K-CSK9-UCS-404	Cisco	Nexus 1000V VSM Virtual Appliance Software On UCS	32
N1K-VLEM-UCS-1	N1K-VLEM-UCS-1	Cisco	Nexus 1000V License PAK For 1 Virtual Ethernet Module On UCS	32
N20-AC0002	N20-AC0002	Cisco	UCS M81KR Virtual Interface Card/PCIe/2-port 10Gb	32
N20-B6625-1	N20-B6625-1	Cisco	UCS B200 M2 Blade Server w/o CPU, memory, HDD, mezzanine	32
N20-BHTS1	N20-BHTS1	Cisco	CPU heat sink for UCS B200 Blade Server	64
N20-C6508	N20-C6508	Cisco	UCS 5108 Blade Server Chassis/0 PSU/8 fans/0 fabric extender	4
N20-FAN5	N20-FAN5	Cisco	Fan module for UCS 5108	32
N20-FW005	N20-FW005	Cisco	UCS 5108 Blade Server Chassis FW package	4

N20-I6584	N20-I6584	Cisco	UCS 2104XP Fabric Extender/4 external 10Gb ports	8
N20-PAC5-2500W	N20-PAC5-2500W	Cisco	2500W power supply unit for UCS 5108	16
SFP-H10GB-CU1M	SFP-H10GB-CU1M	Cisco	10GBASE-CU SFP+ Cable 1 Meter	32
SFP-H10GB-CU3M	SFP-H10GB-CU3M	Cisco	10GBASE-CU SFP+ Cable 3 Meter	96
UCS-VMW-N1K-BUN	UCS-VMW-N1K-BUN	Cisco	Bundle of VMware Ent Plus and Nexus 1K License	32
VMW-VCS-1A	VMW-VCS-1A	Cisco	VMware vCenter Server Standard, 1yr support required	32
VMW-VS-ENTP-3A	VMW-VS-ENTP-3A	Cisco	VMware vSphere Enterprise Plus (1 CPU), 3yr support required	32

Data Center—Core

Name	Catalog Num	Vendor	Description	Qty
N7K-C7010-BUN-R	N7K-C7010-BUN-R	Cisco	Nexus 7010 Bundle (Chassis,(2)SUP1,(3)FAB1,(3)AC-6KW PSU)	1
N7K-AC-6.0KW	N7K-AC-6.0KW	Cisco	Nexus 7000 - 6.0KW AC Power Supply Module	3
N7K-C7010-FAB1-BUN	N7K-C7010-FAB1-BUN	Cisco	Nexus 7000 - 10 Slot Chassis - 46Gbps/Slot Fabric Module	3
N7K-SUP1-BUN	N7K-SUP1-BUN	Cisco	Nexus 7000 - Supervisor 1, Includes External 8GB Flash	2
CAB-AC-2500W-US1	CAB-AC-2500W-US1	Cisco	Power Cord, 250Vac 16A, straight blade NEMA 6-20 plug, US	6
CON-SNTP-C701BR	CON-SNTP-C701BR	Cisco	SMARTNET 24X7X4 Nexus 7010 Bundle	1
N7K-M132XP-12	N7K-M132XP-12	Cisco	Nexus 7000 - 32 Port 10GbE, 80G Fabric (req. SFP+)	3
N7K-M148GT-11	N7K-M148GT-11	Cisco	Nexus 7000 - 48 Port 10/100/1000, RJ-45	1
N7KS1K9-50	N7KS1K9-50	Cisco	Cisco NX-OS Release 5.0	1
N7K-C7010-BUN-R	N7K-C7010-BUN-R	Cisco	Nexus 7010 Bundle (Chassis,(2)SUP1,(3)FAB1,(3)AC-6KW PSU)	1
N7K-AC-6.0KW	N7K-AC-6.0KW	Cisco	Nexus 7000 - 6.0KW AC Power Supply Module	3

N7K-C7010-FAB1-BUN	N7K-C7010-FAB1-BUN	Cisco	Nexus 7000 - 10 Slot Chassis - 46Gbps/Slot Fabric Module	3
N7K-SUP1-BUN	N7K-SUP1-BUN	Cisco	Nexus 7000 - Supervisor 1, Includes External 8GB Flash	2
CAB-AC-2500W-US1	CAB-AC-2500W-US1	Cisco	Power Cord, 250Vac 16A, straight blade NEMA 6-20 plug, US	6
CON-SNTP-C701BR	CON-SNTP-C701BR	Cisco	SMARTNET 24X7X4 Nexus 7010 Bundle	1
N7K-M132XP-12	N7K-M132XP-12	Cisco	Nexus 7000 - 32 Port 10GbE, 80G Fabric (req. SFP+)	3
N7K-M148GT-11	N7K-M148GT-11	Cisco	Nexus 7000 - 48 Port 10/100/1000, RJ-45	1
N7KS1K9-50	N7KS1K9-50	Cisco	Cisco NX-OS Release 5.0	1

APPENDIX B

Cisco Products and Software Versions

	Device DNS Name	Model	Current Software
Branches			
	FW-A2-MSP-1	ASA5515-x	asa900-129-smp-k8.bin
	R-A2-Conv-1	CISCO891W	c890-universalk9-mz.151-3.T.bin
	R-A2-Mini-1	CISCO1941W-A/K9	c1900-universalk9-mz.SPA.151-3.T.bin
	R-A2-Small-1	CISCO2921/K9	c2900-universalk9-mz.SPA.151-3.T.bin
	R-A2-Med-1	CISCO2951 (STARSCREAM Rev 1)	c2951-universalk9-mz.SPA.151-3.T.bin
	R-A2-Med-2	CISCO2951/K9	c2951-universalk9-mz.SPA.151-3.T.bin
	R-A2-Lrg-1	C3945-SPE150/K9	c3900-universalk9-mz.SPA.151-3.T.bin
	R-A2-Lrg-2	C3945-SPE150/K9	c3900-universalk9-mz.SPA.151-3.T.bin
Internet Edge			
	RIE-1	ASR-1002X	asr1002x-universalk9.03.08.00.S.153-1.S.SPA.bin
	RIE-2	ASR-1002X	asr1002x-universalk9.03.08.00.S.153-1.S.SPA.bin
	RIE-3	Catalyst6509-Sup720-3BXL	s72033-adventerprisek9_wan-mz.122-33.SXI5.bin
	RIE-3_ASASM	WS-SVC-ASA-SM1-K9	asa911-smp-k8.bin / asdm-711.bin
	RIE-3_IDSM	WS-SVC-IDSM-2	7.0(4)
	RIE-3_ACE	ACE30-MOD-K9	c6ace-t1k9-mz.A5_2_1.bin
	RIE-4	Catalyst6509-Sup720-3BXL	s72033-adventerprisek9_wan-mz.122-33.SXI5.bin
	RIE-4_ASASM	WS-SVC-ASA-SM1-K9	asa911-smp-k8.bin / asdm-711.bin
	RIE-4_IDSM	WS-SVC-IDSM-2	7.0(4)
	RIE-4_ACE	ACE30-MOD-K9	c6ace-t1k9-mz.A5_2_1.bin
	ASA-IE-1	ASA5540 w/SSM-40	asa841-k8.bin
	ASA-IE-2	ASA5540 w/SSM-CSC-10	asa841-k8.bin

	IRONPort	Ironport C670	v7.1.3-010
Data Center			
	RWAN-1	ASR-1002 (RP1)	asr1000rp1-adventerprisek9.03.02.01.S.151-1.S1.bin
	RWAN-2	ASR-1002 (RP1)	asr1000rp1-adventerprisek9.03.02.01.S.151-1.S1.bin
	ASA-WAN-1	ASA5515-X	asa911-smp-k8.bin / asdm-711.bin
	ASA-WAN-2	ASA5515-X	asa911-smp-k8.bin / asdm-711.bin
	RCORE-1	Catalyst6509-Sup720-3BXL	s72033-adventerprisek9_wan-mz.122-33.SXJ.bin
	RCORE-2	Catalyst6509-Sup720-3BXL	s72033-adventerprisek9_wan-mz.122-33.SXJ.bin
	RAGG-1	C7010 Chassis ("Supervisor module-1X")	n7000-s1-dk9.5.1.2.bin
	RAGG-1_VDC1	C7010 Chassis ("Supervisor module-1X")	n7000-s1-dk9.5.1.2.bin
	RAGG-1_VDC2	C7010 Chassis ("Supervisor module-1X")	n7000-s1-dk9.5.1.2.bin
	RAGG-2	C7010 Chassis ("Supervisor module-1X")	n7000-s1-dk9.5.1.2.bin
	RAGG-2_VDC1	C7010 Chassis ("Supervisor module-1X")	n7000-s1-dk9.5.1.2.bin
	RAGG-2_VDC2	C7010 Chassis ("Supervisor module-1X")	n7000-s1-dk9.5.1.2.bin
	DC-ASA-1_Admin	ASA-5585	asa824-smp-k8.bin
	DC-ASA-1_VDC1	ASA-5585	asa824-smp-k8.bin
	DC-ASA-1_VDC2	ASA-5585	asa824-smp-k8.bin
	DC-ASA-2_Admin	ASA-5585	asa824-smp-k8.bin
	DC-ASA-2_VDC1	ASA-5585	asa824-smp-k8.bin
	DC-ASA-2_VDC2	ASA-5585	asa824-smp-k8.bin
	RSERV-1	Catalyst6509-Sup720-3BXL	s72033-adventerprisek9_wan-mz.122-33.SXJ.bin
	RSERV-1_IDSM	WS-SVC-IDSM-2	7.0(4)
	RSERV-1_ACE	ACE30-MOD-K9	c6ace-t1k9-mz.A5_2_1.bin
	RSERV-2	Catalyst6509-Sup720-3BXL	s72033-adventerprisek9_wan-mz.122-33.SXJ.bin
	RSERV-2_IDSM	WS-SVC-IDSM-2	7.0(4)
	RSERV-2_ACE	ACE30-MOD-K9	c6ace-t1k9-mz.A5_2_1.bin
Branches			
	S-A2-MSP-1	WS-C2960S-48FPD-L	c2960s-universalk9-mz.122-53.SE2.bin
	A-A2-MSP-1	AIR-CAP3502I	
	S-A2-Conv-1	WS-C2960PD-8TT-L	c2960-lanbasek9-mz.122-55.SE1.bin

	S-A2-Mini-1	WS-C2960G-8TC-L	c2960-lanbasek9-mz.122-50.SE4.bin
	S-A2-Mini-2	WS-C2960-8TC-L	c2960-lanbasek9-mz.122-50.SE4.bin
	A-A2-Mini-1	AIR-CAP3502E	
	S-A2-Small-1	WS-C2960S-48FPS-L	c2960s-universalk9-mz.122-53.SE1.bin
	S-A2-Small-2 (Stacked)	WS-C2960S-48FPS-L	c2960s-universalk9-mz.122-53.SE1.bin
	A-A2-Small-1	AIR-CAP3502I	
	S-A2-Med-1	WS-C3750X-48PF-S	c3750e-universalk9-mz.122-53.SE2.bin
	S-A2-Med-2 (Stacked)	WS-C3750X-48PF-S	c3750e-universalk9-mz.122-53.SE2.bin
	S-A2-Med-3	WS-C2960CPD-8PT-L	c2960c405-universalk9-mz.122-55.0.43.SK.bin
	A-A2-Med-1	AIR-CAP3502E	
	A-A2-Med-2	AIR-LAP1262N	
	S-A2-Lrg-1	WS-4507+R SUP-7	cat4500e-universalk9.SPA.03.01.00.SG.150-1.XO.bin
	S-A2-Lrg-2	WS-4507+R SUP-7	cat4500e-universalk9.SPA.03.01.00.SG.150-1.XO.bin
	S-A2-Lrg-3	WS-C3560X-48PF-S	c3560e-universalk9-mz.122-53.SE2.bin
	S-A2-Lrg-4	WS-C3560X-48PF-S	c3560e-universalk9-mz.122-53.SE2.bin
	S-A2-Lrg-5	WS-C3560CPD-8PT-L	c3560c405ex-universalk9-mz.122-55.0.44.SK.bin
	A-A2-Lrg-1	AIR-CAP3502E	
	A-A2-Lrg-2	AIR-CAP3502I	
	SLC-A2-Lrg-1	AIR-CT5508-12-K9	7.0.114.112
	WAVE-A2-Lrg-1	WAVE-547	
Data Center			
	SWAN-1/2	WS-C3750X-48PF-S	c3750e-universalk9-mz.122-53.SE2.bin
	SWAN-3/4	WS-C3750X-48PF-S	c3750e-universalk9-mz.122-53.SE2.bin
	SACCESS-1	WS-C3750X-48PF-S	c3750e-universalk9-mz.122-53.SE2.bin
	SACCESS-2	WS-C3750X-48PF-S	c3750e-universalk9-mz.122-53.SE2.bin
	SACCESS-3	Nexus5020 Chassis ("40x10GE/Supervisor")	n5000-uk9.5.0.3.N1.1b.bin
	SACCESS-4	Nexus5020 Chassis ("40x10GE/Supervisor")	n5000-uk9.5.0.3.N1.1b.bin
	SACCESS-5	WS-C3750X-48P	c3750e-universalk9-mz.122-53.SE2.bin
	F-UCS-1	UCS6120-Fabric	4.1(3)N2(1.3p)
	F-UCS-2	UCS6120-Fabric	4.1(3)N2(1.3p)
	MDS-DC-1	MDS 9506 ("Supervisor/Fabric-2")	m9500-sf2ek9-mzg.5.0.1a.bin.S4
	MDS-DC-2	MDS 9506 ("Supervisor/Fabric-2")	m9500-sf2ek9-mz.5.0.4.bin
	AW-DC-1	AIR-WLC5508-12	7.0.114.112

	AW-DC-2	AIR-WLC5508-12	7.0.114.112
	MSE-DC-1	MSE3550	7.0.200.125
	MSE-DC-2	MSE3550	7.0.200.125
	Nexus 1kv	Nexus 1kv	4.2(1)SV1(4)
	Nexus VSG	Nexus VSG	4.2(1)VSG1(1)
	Cisco ISE	Cisco Identity Service Engine	1.2
	WCS Manager	Cisco WCS Manager	7.0.171.107
	CS Manager	Cisco Security Manager	4.0.1
	CS ACS	Cisco Secure Access Control Server	Release 4.2(1) Build 15 Patch 3
	Cisco Prime LMS	Cisco Prime Lan Management Solution	version 4.2.2 with NCM/Pari
	Cisco UCS Manager	Cisco UCS Manager	1.3(1p)
	Cisco UCM	Cisco Unified Communications Manager	8.5.1.11001-3
	EMC UIM	EMC Unified Infrastructure Manager'	2.0.1.1.160
	EMC Unisphere	EMC Unisphere	1.0.50.1.0326
	RSA DPM	RSA Data Protection Manager	KM-3.1 / AM-6.1.SP3
	RSA enVision	RSA enVision	RSA enVision 4.0 , Revision 5
	RSA Authentication Manager	RSA Authentication Manager	7.1 Service Pack 2
	RSA Archer	RSA Archer	4.5.5
	HyTrust	HyTrust	2.2.1.14064
	VSOM	Cisco Video Surveliance Manager	6.3.1
	PAM	Cisco Physical Access Manager	1.2.0

APPENDIX C

Reference Architecture Assessment Report—Cisco Healthcare Solution

Based on: Healthcare Information Portability and Accountability Act of 1996 (HIPAA Security Rule)

November 27, 2013

Contact Information

Verizon Business **Kenneth Luberto** *Sr. Security Consultant* kenneth.luberto@one.verizon.com **Larry Bickner** *Principal Security Consultant* larry.k.bickner@one.verizon.com	
Cisco Systems, Inc. **Christian Janoff** *Compliance Solutions Architect* christian.janoff@cisco.com **Bart McGlothin** *Compliance Solutions Architect* bart.mcglothin@cisco.com	

Table of Contents

1. Executive Summary 2
2. Introduction 5
Reference Documentation 5
Business Associate 6
Timeframe 6
Cisco's Healthcare Reference Architecture 7
Reference Model Components 8
Network Segmentation and Management 9
Wireless LANs and/or Wireless Applications 9
3. Assessment Findings and Conclusions 10
3.1 Safeguard Exclusions 10
3.2 Safeguards Provided throughout the Reference Model 16
4. Safeguard Mapping to Security Control Areas 18
5. Control Mapping to Cisco's Healthcare Reference Architecture 24
6. Application of the Healthcare Reference Architecture 26
7. Appendix 28
Healthcare Security Requirements 28
List of Interviews 30
List of Documents 31

1. Executive Summary

Cisco Systems, Inc. (Cisco) engaged Verizon's Global Consulting and Integration Services (GCIS) to conduct a security controls assessment (Assessment) of Cisco's "Healthcare Solution" designed architecture, based on maximizing the alignment of Cisco's available security controls with the Healthcare Information Portability and Accountability Act (HIPAA) Security Rule safeguards. This Assessment reviewed how Cisco's "reference security architecture" provided either direct security controls or compensating security controls, which are capable of meeting or exceeding the security "safeguards" as identified in HIPAA. This Assessment included the review of Cisco's reference security architecture and the user, data, network, and system controls provided therein.

Cisco markets the assessed reference architecture solution to their customers looking to meet their healthcare security requirements, specifically within their IT environment and within their data center infrastructure. Cisco will use the findings from this assessment to design a solution that aligns with the security requirements that are generally accepted to fulfill security controls, with respect to the HIPAA security safeguards (requirements), and plan to provide the results of this Assessment to Cisco Sales Engineers interfacing with their enterprise Customers.

Verizon's Assessment covered Cisco's enterprise architectures including: datacenter; Internet edge; WAN; small, medium, and large clinic architectures; clinics/out-patient facilities; and small hospitals, among others.

The Cisco reference architecture is not designed or envisioned to directly fulfill the HIPAA Safeguards that are purely operational or organizational (for example, the assignment of the HIPAA Security Officer), or purely documentation oriented (for example, the assurance that documents are regularly reviewed). Verizon has found that Cisco's reference architecture for Healthcare does provide a strong technology foundation for managing technical risks that meet the healthcare customer's need to manage risks, specifically around the protection of electronic Patient Health Information (ePHI).

The Healthcare Security Requirements revolve around HIPAA Part 164 Part C. HIPAA Part 164 Subpart C is made up of nine sections. Three of the sections are administrative and are not part of this assessment. The remaining six sections (Security Standards: General Rules; Administrative Safeguards; Physical Safeguards; Technical Safeguards; Organizational Requirements; and Policies and Procedures and Documentation Requirements) consist of **52** Security Safeguards. Verizon performed an initial assessment to determine whether the safeguards could be met by using specific technology components provided by Cisco.

Of the **52** Safeguards in the current healthcare requirements, Verizon identified **29 Safeguards as not applicable** in the context of this Assessment, because the Safeguard was either explicit and demanding direct (non-technology related) controls, or general but not allowing for the reasonable use of technology as a compensating control in the fulfillment of the Safeguard.

Of the remaining 23 Safeguard Areas in the current healthcare requirements, Verizon has further identified **8 Safeguards that call for universal security control requirements** that are foundational across Cisco's products and present in all network devices and systems that make up Cisco's Healthcare Reference Architecture.

Safeguard Areas where Cisco Security Controls are Not-Applicable	Safeguard Areas where Cisco Security Controls are Universally Applicable	Safeguard Areas where Cisco Security Controls are Specifically Applicable
29	8	15

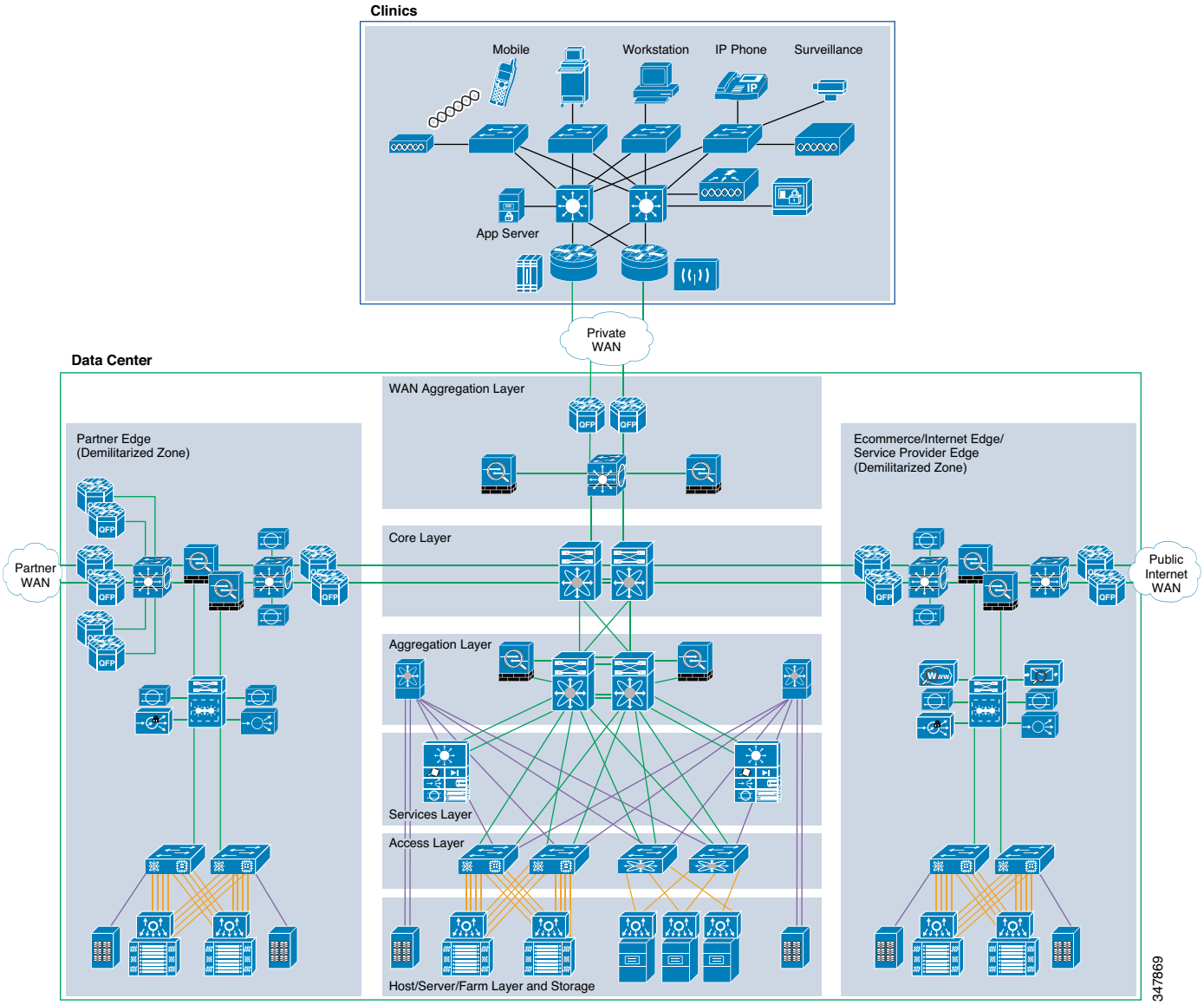
In the remaining 15 Safeguard Areas in the current healthcare requirements, Verizon assessed the capability and capacity for Cisco's Healthcare Reference Model to support technically Direct Control that meet the intent of the Safeguard, or to provide Compensating Controls that, when implemented in conjunction with layered controls, the Healthcare Reference Model could support the fulfillment of the Safeguard; as a technology implementation that would in turn allow for a less complex operating procedure or management process to meet this Safeguard. Verizon has identified the primary security controls that could be used to form a technical foundation of direct and compensating controls, for complying with the healthcare requirements.

Based on our assessment, Verizon believes that Cisco's Healthcare Reference Architecture provides a robust networking core and infrastructure that can support a customer's implementation of network security controls and system security controls as part of their security program and as a required HIPAA-Required Risk Management process. The architecture also provides both strong common security controls through network devices and security control and management systems that are highly capable to support data security, and specific security management components that are directly applicable to meet HIPAA safeguard control requirements. The fact that Cisco devices universally support the core security controls outlined in HIPAA Safeguards allows a customer to implement the reference architecture with the confidence that their resulting infrastructure will support HIPAA compliance from the outset, and with the knowledge that any additional use of Cisco's security management tools will only enhance the protection of ePHI and further support Healthcare compliance.

Cisco's Healthcare Reference Architecture also provides directly applicable security control features and capabilities owing to the depth of security management tools provided in this model. Directly Applicable controls include: Physical Access Control, Intrusion Detection, and Visual Surveillance;

Network Access and Authentication Controls for wired, wireless, and remote networks; Network Segmentation, Segregation, and Isolation Capabilities; Logging, Auditing, and Monitoring Capabilities; and Encryption.

Figure C-1 Enterprise-wide Healthcare Reference Architecture



2. Introduction

Reference Documentation

HIPAA (the "Act") was signed into law in 1996 (Public Law 104-191). Title II (Fraud, Simplification, and Abuse) of the Act contains the Administrative Simplification provisions with which Covered Entities (CEs) must comply in order to facilitate the exchange of electronic Protected Health Information (ePHI) and to ensure the security and confidentiality of consumer information. The Act asserts that CEs that collect, store, and/or process PHI in electronic form must make a good faith effort to protect the corporate computing environment from reasonably anticipated threats and vulnerabilities, and take reasonable and appropriate measures to protect the integrity, confidentiality, and security of such electronic data. The security protections selected may be examined in the event that the CE and its associated business partners and service providers are the subjects of a compliance audit.

The HIPAA Security Final Rule that implements the Act requires CEs to perform an analysis of the potential risks to the electronic PHI for which they are responsible; and then develop, implement, and maintain appropriate security measures to safeguard the integrity, confidentiality, and availability of that data. Security plans must fully document the security measures implemented by the organization and should reflect the management of risk to acceptable levels. Periodic evaluation of the risks to the corporate computing environment and ePHI is also a requirement.

The HIPAA Security Final Rule is a regulatory framework that incorporates recognized security objectives and protections, but which is intentionally technology-neutral. The Final Rule provides standards and, in some cases, implementation specifications, that require CEs to implement predetermined controls. To achieve a baseline level of compliance, a covered entity must have a comprehensive information security program. The scope and nature of each covered entity's security program will vary according to its specific environment and associated vulnerabilities as determined through its risk analytical processes. Although the standard is objective, a covered entity's specific security controls may vary, as the Final Rule permits flexibility in approach to compliance. The Final Rule permits CEs to select "reasonable and appropriate" control measures according to level of risk and potential tolerance within the environment. For example, CEs can achieve compliance with authentication requirements by using strong passwords or through biometric technology. The choice to implement one authentication tool over another must be based in large part on the likelihood a security breach will occur and the potential damage that could result from such a breach.

HIPAA consists of three main Parts (sections) that are designed to put in place security and privacy requirements for protection of Protected Health Information (PHI). Each Part has multiple subparts that provide detail for the section.

- Part 160—General Administrative Requirements: Deals mostly with the legal, compliance, and penalty aspects of HIPAA.
- Part 162—Administrative Requirements: Deals with unique identifiers for Covered Entities in Healthcare, provisions for transactions, and many other administrative issues in Healthcare.
- Part 164—Security and Privacy: Deals with the Safeguards for protecting PHI in electronic and paper media. This section is generally broken down into General Provisions §164.1xx, Security Standards for the Protection of Electronic Protected Health Information §164.3xx, Notification in Case of Breach of Unsecured Protected Health Information §164.4xx and Privacy of Individually Identifiable Health Information §164.5xx. This report deals mainly with the Security Standards for the Protection of Electronic Protected Health Information Subpart C.

There have been multiple discussions surrounding the required security components an organization needs to implement in order to meet HIPAA guidelines. Specific technologies such as intrusion detection and firewalls are not mandated and implementing appropriate security controls to address the requirements are determined by the covered entity.

HIPAA as written includes a flexibility rule in the security standards for determining the appropriate security controls based on a covered entities size, technical infrastructure, and hardware and software capabilities. Under §164.306 Security Standards: General Rules it states:

> (b) Flexibility of approach.
>
> (1) Covered entities and business associates may use any security that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.
>
> (2) In deciding which security to use, a covered entity or business associate must take into account the following factors:
>
> (i) The size, complexity, and capabilities of the covered entity or business associate.
>
> (ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities.
>
> (iii) The costs of security measures.
>
> (iv) The probability and criticality of potential risks to electronic protected health information.

This flexibility has led to confusion on occasion as covered entities attempt to identify appropriate security controls for their organization. Assessors have used current industry-accepted security practices to assess the security controls to determine the level of compliance with the safeguards. Typical infrastructure components such as firewalls, intrusion detection/ prevention, and network segmentation are among the technical controls that are industry-accepted security practices assessors typically review.

Business Associate

While HIPAA was written for CEs, consideration was taken into account for partners or Business Associates (BAs) that provide services to the CEs. The U.S. Department of Health and Human Services description of a business associate is: A “business associate” is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. Further the American Reinvestment and Recovery Act (ARRA) of 2009 and the recent Omnibus Ruling in 2013 placed additional requirements on BAs to implement controls to meet HIPAA Security requirements. This significantly expands the HIPAA security requirements to organizations outside of the healthcare field. Organizations failing to meet the requirements are subject to substantial financial penalties.

Timeframe

Verizon performed this assessment in Q1 and Q2 of 2013. The previous PCI assessment which was performed in 2012 was used as a reference to gather knowledge about Cisco product offerings and to review the reference architecture.

Cisco's Healthcare Reference Architecture

Cisco's Healthcare reference architecture supports the networking infrastructure commonly seen in national-level healthcare organizations down to individual clinics operating as part of a regional health group. The architecture supports the centralization of ePHI into regional data centers (i.e. in hospitals or regional data center facilities) or into a central (national data center with regional backups).

The Architecture supports data, system, and application segmentation, segregation, and isolation at the data center level to allow for structuring of systems/network segments containing ePHI (for example, clinical systems) from networks/workstations/systems not intended for ePHI processing or storage (for example, administrative systems). The architecture addresses Internet isolation and patient access, remote secure access into the infrastructure by authenticated users, and the stratification of clinics, administrative offices, hospitals, and out-patient facilities that each have a variable need for ePHI access.

Reference Model Components

The architecture assessment included the following components:

CISCO COMPONENT	SPECIFIC CISCO DEVICES INCLUDED IN THE REFERENCE MODEL
Cisco Routers (ISR)	891w-AGN, 1941w, ISR G2, 2921/51 ISR G2, 3945 ISR G2, ASR1002, ISRs are configured with Firewall and IDS feature set.
Cisco Firewalls (ASA)	Network Firewall device, ASA-5585-x, ASA-5555-x, ASA-5500, ASA-5515-x
Cisco Switches	2960 PD-8TT-L, 2960- 8TC-L, 2960 S, 2960 C, 3560 C, 3560 X, 3750 X, 4507-Sup 7, 6500, Nexus1000v, Nexus5000, Nexus7000, MDS 9500, Catalyst-2000, Catalyst-3000, Catalyst-4000, Catalyst-6000
MDS Switch Fabric	
Cisco Wireless	1262N Access Points, 3502E Access Points, 3502I Access Points, CT5508 Controller, WLC2125 Controller, Mobility Service Engine, WCS-Wireless Manager, AIR-XXX, 891W, 1941W
Cisco Security devices	ASA 5585, ASA 5555, ASA 5515-x, NAC, IOS Firewall, AnyConnect - VPN. Catalyst ASA Services Module, Catalyst Intrusion Detection Service Module
Server Vitalization	Servers - ISR SRE 900, UCS Express server ESXi
VBlock	UCS - MDS - EMC SAN, EMC-Clarion,
Cisco Security Manager	Central provisioning of device configuration and security policies, including: ASAs, Cisco ASA Services Modules, IDS, ISRs, and switches
Cisco Secure Access Control Server (ACS)	AAA server
Cisco Prime LAN Management Solution (LMS)	Configuration Management / Configuration Enforcement and monitoring (Pari Compliance Module)
Cisco Physical Access Manager (PAM)	Configuration and central management of Cisco physical access control devices
Cisco Physical Access Gateway	Primary controlling device for physical access
Cisco Identity Services Engine (ISE)	Central Authentication, Policy / Configuration enforcement
RSA Access Manager	Used for central authentication/logging for access to RSA Data Protection Manager within the assessed environment.
RSA Authentication Manager	Central management/logging of RSA SecurID (two-factor) authentication for remote access into the data center environment.
RSA Data Protection Manager	formerly RSA Key Manager
RSA enVision	RSA's solution for compliance and security information management. RSA enVision was used to centrally collect RSA SecurID authentication logs on the RSA Authentication Manager server, using a batch process that runs several times a day.
HyTrust	Network-based virtual infrastructure policy enforcement. Administrative access control, enforcement of policy across virtual infrastructure, hypervisor hardening, and audit logging. Access and User administration, change and configuration, and operations

Network Segmentation and Management

Cisco has designed several network architectures to account for small, medium, and large healthcare IT environments. Cisco chose Integrated Services Routers (ISRs) to provide firewall, IDS, and routing functionality. Access-lists are applied through firewall policies, which are pushed to the ISRs in each architecture. Access-lists implicitly deny all inbound and outbound traffic across the network; Approved traffic must be explicitly allowed to the IP address, port and service level thereby creating access control granularity. Additionally, Cisco has incorporated wireless into the design, using WPA2, WPA-TKIP for secure wireless networking to support seamless control strategies for both wireless and wired networks.

The data center environment is segmented into multiple VLANs, including Internet Edge, WAN aggregation, and Core service aggregation. Multiple layers of network security are included in each data center segment, including Cisco ASA Services Module and ASA stateful firewall filtering and integrated IDS/ detection/prevention, access lists, secure VPN (WAN aggregation and remote VPN), and two-factor authentication. These devices allow for fine-grained control of network and system access between systems, and support isolating ePHI-containing systems/servers from IT resources that need not be exposed to ePHI. (e.g. Administrative systems) Network devices are centrally managed through the following:

- Cisco Security Manager (CSM)—(Central security management for ISRs and switches (e.g., firewall policy, IDS/signatures)
- Cisco Wireless Control System (WCS)—Central wireless management
- Cisco ACS—Central TACACS+ (central authentication) server for ASA firewall, Cisco ASA Services Module, ISR, ASR router, switch, wireless controller (RSA enVision and WCS).
- RSA enVision—Central logging/Correlation/Analysis/Alerting server. Alerts from IDS/alerts and firewall logs.
- Cisco ASDM—configuration for ASA firewalls.
- Cisco Device Manager (IDM)—IDS/configuration management.
- Cisco Prime LAN Management Solution (LMS)—Central configuration management, monitoring, and troubleshooting.
- Cisco Identity Services Engine (ISE) – Central Authentication, Policy / Configuration enforcement for ASA firewall, Cisco ASASM, ISR / VXR routers, Cisco switch, and wireless controllers

Wireless LANs and/or Wireless Applications

Wireless networks within the reference environment are configured to use WPA2, WPA-TKIP authentication for secure wireless networking. Wireless traffic must pass through the ISRs and IOS firewall access-lists to traverse any part of the network, thereby controlling wireless access to network segments and devices containing ePHI. Best practice security parameters have been applied to wireless networks, including: HTTPS access for wireless management, default SSID has been changed, SNMPv3 used (default strings changed), and HTTP access has been disabled.

Wireless technology in the PHI environment is a growing concern for organizations in the healthcare field. Implementing wireless requires that appropriate security controls are in place to prevent, detect, and respond to security violations. Appropriate controls include implementing a firewall to segment and protect the PHI data environment and intrusion detection services to identify potential intrusion attempts to the secured network. Encryption must be configured to adequately protect PHI transmitted over the wireless medium.

3. Assessment Findings and Conclusions

The Healthcare Security Requirements revolve around HIPAA Part 164 Part C. HIPAA Part 164 Subpart C is made up of nine sections. Three of the sections are administrative and are not part of this assessment. The remaining six sections consist of 52 Security Safeguards. Verizon performed an initial assessment to determine whether the safeguards could be met by using specific technology components provided by Cisco.

3.1 Safeguard Exclusions

Of the 52 Safeguard Areas in the current healthcare requirements, Verizon identified 29 Safeguards as not applicable in the context of this Assessment because the Safeguard was either explicit and demanding direct (non-technology related) controls, or general but not allowing for the reasonable use of technology as a compensating control in the fulfillment of the Safeguard. The Safeguards deemed as non-applicable under this assessment, and thereby removed for further consideration, include. the following.

Citation	Safeguard Title	Safeguard Description	Applicability of Technical Solutions to this Safeguard
§164.308(a)(1)(ii)(C)	Risk Analysis	Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to ePHI held by the covered entity or business associate.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. - This Safeguard calls for a risk assessment to identify all areas of risk to ePHI. All infrastructure components that process, store or transmit ePHI must be addressed.
§164.308(a)(1)(ii)(C)	Risk Management	Implement security measures to sufficiently reduce the risks and vulnerabilities to a reasonable and appropriate level.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. - This Safeguard calls for the implementation of appropriate controls to address the risks identified in the risk assessment. Technological controls for each infrastructure component need to be evaluated to determine if they can appropriately protect ePHI.
§164.308(a)(1)(ii)(C)	Sanction Policy (1)(ii)(C)	Ensure that sanctions are in place to discipline workforce members of the covered entity or business associate who fail to comply with the security policies and procedures for protecting ePHI.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. - This Safeguard calls for the implementation of an operating Policy with the Customer's environment, and while a strong technical security baseline can support implementation of the Policy, it cannot substitute for a written policy that is distributed across the workforce.

§164.308(a)(2)	Assigned security responsibility	Assign responsibility for the development and implementation of the policies and procedures for protecting ePHI required by the covered entity and business associates.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. - This safeguard calls for the covered entity to formally assign an individual who is responsibility for the security program development and implementation of appropriate policies and procedures to protect ePHI. This is a personnel issue only and there is no technology requirements directly affiliated with this safeguard.
§164.308(a)(3)(ii)(B)	Workforce Clearance Procedure	Implement policies and procedures to determine that access of workforce members to ePHI is appropriate.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard is looking for a policy and procedure to ensure that access to ePHI is appropriate. While technical controls may be used implement the policy, it Is not the direct intent of this safeguard.
§164.308(a)(5)(ii)(A)	Security Reminders	Identify and distribute periodic security updates to all members of the workforce including management.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard is looking to ensure that policies and procedures are in place for the occasional distribution of security reminders to reinforce or update all staff on new threats and vulnerabilities.
§164.308(a)(7)(ii)(A)	Data Backup Plan	Establish and implement procedures to create and maintain retrievable copies of ePHI.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. -This Safeguard calls for backing up data and storing copies off-site that can be retrieved in response to an emergency that damages systems that contain ePHI.
§164.308(a)(7)(ii)(B)	Disaster Recovery Plan	Establish and implement procedures to restore any loss of ePHI data.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. - This Safeguard calls for a documented plan to restore any loss of ePHI data.
§164.308(a)(7)(ii)(D)	Testing and Revision Procedures	Implement procedures for periodic testing and revision of contingency plans.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This Safeguard calls for the periodic testing and revision of the disaster recovery plan.

§164.308(a)(7)(ii)(E)	Applications and Data Criticality	Assess the relative criticality of specific applications and data in support of other contingency plan components.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This Safeguard calls for the criticality of each application to be assessed to determine the priority required to restore applications in an emergency.
§164.308(b)(1)	Business Associate Contracts	Each covered entity is required to obtain satisfactory assurances that business associates that create, receive or maintain or transmit ePHI on the covered entities behalf will appropriately safeguard the information in accordance with HIPAA regulations.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. - This safeguard calls for contractual assurances (legal) that ePHI will be appropriately protected when in custody of a business associate of the covered entity.
§164.310(a)(2)(i)	Contingency Operation	Establish and implement procedures that allow for facility access in support of restoration of lost data under disaster recovery plan and emergency access mode operations.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This Safeguard calls for policies and procedures that allow for access to the facilities to restore lost data during a disaster or emergency.
§164.310(a)(2)(ii)	Facility Security Plan	Implement policies and procedures to safeguard the facility and the equipment inside from physical access, tampering and theft.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. - This safeguard is looking to ensure that physical access is available to authorized personnel to support the restoration of lost data in contingency operations
§164.310(a)(2)(iv)	Facility Access Controls - Maintenance Records	Description: Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard is looking to ensure that devices providing physical security are maintained to prevent failure and allow unauthorized physical access to the facilities that process, store or transmit ePHI.

§164.310(b)	Workstation Use-Workstation Use	Description: Implement policies and procedures that specify the proper functions and the physical attributes for workstations that can access ePHI.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard is looking to ensure that all employees or contractors that have access to a workstation that has or may have access to ePHI is aware of the appropriate use of the workstation.
§164.310(c)	Workstation Security-Workstation Security	Description: Implement physical safeguards for all workstations that access ePHI.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard is looking to ensure that all workstations that have or may have access to ePHI are appropriately secured to prevent unauthorized access.
164.310(d)(2)(i)	Device and Media Controls- Device and Media Disposal	Description: Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard is looking to ensure that policies and procedures are in place remove ePHI from devices and media before disposal.
§164.310(d)(2)(ii)	Device and Media Controls- Media Re-Use	Description: Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard is looking to ensure that policies and procedures are in place remove ePHI from devices and media before they are re-used.
§164.310(d)(2)(iii)	Accountability - Asset Ownership and Location	Assign responsibility for recording and maintaining the movement of hardware and electronic media that contain ePHI.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. - Solution requires Asset and device ownership to identify where assets containing ePHI are located. Designed to ensure that data is not exposed unintentionally.
§164.310(d)(2)(iv)	Device and Media Controls -Data Backup and Storage	Description: Create a retrievable exact copy of ePHI when needed before movement of equipment.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard is looking to ensure that an exact backup copy of ePHI is made before a device is moved.

§164.314(a)(1)	Business Associate Non-Compliance	Each covered entity is required to obtain satisfactory assurances that business associates that create, receive or maintain or transmit ePHI on the covered entities behalf will appropriately safeguard the information in accordance with HIPAA regulations.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard calls for contractual assurances (legal) that ePHI will be appropriately protected when in custody of a business associate of the covered entity.
§164.314(a)(2)(i)	BA Information Security Controls	Each covered entity is required to obtain satisfactory assurances that business associates that create, receive or maintain or transmit ePHI on the covered entities behalf will appropriately safeguard the information in accordance with HIPAA regulations.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard calls for contractual assurances (legal) that ePHI will be appropriately protected when in custody of a business associate of the covered entity.
§164.314(a)(2)(i)	BA Handling of ePHI	Each covered entity is required to obtain satisfactory assurances that business associates that create, receive or maintain or transmit ePHI on the covered entities behalf will appropriately safeguard the information in accordance with HIPAA regulations.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard calls for contractual assurances (legal) that ePHI will be appropriately protected when in custody of a business associate of the covered entity.

§164.314(a)(2)(i)	BA Contracts and Statutory Obligations	Each covered entity is required to obtain satisfactory assurances that business associates that create, receive or maintain or transmit ePHI on the covered entities behalf will appropriately safeguard the information in accordance with HIPAA regulations.	This safeguard does not require strong technical controls to meet the safeguards, it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard calls for contractual assurances (legal) that ePHI will be appropriately protected when in custody of a business associate of the covered entity.
§164.314(b)(1)	Requirements for Group Health Plans	The Group Health Plan is required to ensure that the plan sponsor will reasonably and appropriately Safeguard ePHI created, received, maintained or transmitted.	This safeguard does not require strong technical controls to meet the safeguards; it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard is looking to ensure that the plan sponsor has policies and procedures in place to appropriately protect ePHI received, maintained or transmitted to or by the plan.
§164.316(a)	Policy and Procedures	Implement policies and procedures to comply with the HIPAA regulations.	This safeguard does not require strong technical controls to meet the safeguards; it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard is looking to ensure that reasonable and appropriate policies and procedures are in place to comply with the HIPAA Security Standard.
§164.316(b)(2)	Documentation Time Limit	Retain policies and procedures for 6 years from the data of its creation or the last date it was in effect.	This safeguard does not require strong technical controls to meet the safeguards; it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard is looking to ensure that policies and procedures are retained for 6 years from the date of its creation or the date it was last in effect.

§164.316(b)(2)	Documentation Availability	Ensure that documentation is available to the persons responsible for implementing the procedures.	This safeguard does not require strong technical controls to meet the safeguards; it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard is looking to ensure that policies and procedures are available to the person(s) responsible for implementing the procedures to which the documentation pertains.
§164.316(b)(2)	Documentation Updates	Review documentation periodically and update as needed in response to environmental or operational changes affecting the security of ePHI.	This safeguard does not require strong technical controls to meet the safeguards; it is designed to use policies and procedures to put the appropriate controls in place. Technology controls may be used for the implementation of part of the safeguard. – This safeguard is looking to ensure that policies and procedures are reviewed and periodically updated as needed in response to environmental or operational changes that could affect the security of ePHI.

3.2 Safeguards Provided throughout the Reference Model

Of the remaining 23 Safeguard Areas in the current healthcare requirements, Verizon has further identified 8 Safeguards that call for universal security control requirements that are foundational across Cisco's products and present in all network devices and systems that make up Cisco's Healthcare Reference Architecture. The Safeguards deemed as universally applicable under this assessment are explained here and removed for additional detailed consideration.

Citation	Safeguard Title	Safeguard Description	Applicability of Technical Solutions to this Safeguard
164.308(a)(1)(i)	Security Management Process	Implement policies and procedures to prevent, detect, contain and correct security violations.	Cisco devices provide security to help an organization prevent, detect and contain security violations. When combining multiple devices in the design guide, multiple levels of security can be put in place to help an organization meet the security requirements of HIPAA.

§164.308(a)(5)(i)	Protection from Malicious Software (5)(ii)(B)	Ensure that appropriate protections against malicious software are in place.	Patch management and protection from malicious software is a hallmark of Cisco's vulnerability management process and services provided around all Cisco products. Cisco continually reviews potential network, systems and applications threat, attack vectors being used to attempt to penetrate network and systems services, assesses the applicability of these attacks to Cisco products, and, as warranted, issues software patches and improvements to continually stay in front of the impact of malicious software or attacks. Additionally, Cisco firewalls and routers provide network segmentation that can help contain malicious software to a network segment.
§164.308(a)(5)(i)	Password Management (5)(ii)(D)	Ensure that appropriate policies and procedures are in place to manage passwords for network access and access to sensitive data to ensure that passwords are strong enough to prevent them from being guessed or exposed to brute force attacks and processes are in place to manage and protect passwords from compromise or exposure.	Cisco systems and devices all use strong passwords in support of this requirement. Passwords can be configured for AES encryption during transit and in storage providing a higher layer of security and preventing password theft by physical compromise of the device. Administrator passwords can be set to match current industry accepted practices for length, complexity, history, lifetime, failed login attempts and can be authenticated using TACACS or Active Directory.
§164.308(a)(8)	Periodic Technical and Non-Technical Evaluation	Ensure that periodic technical (pen/vulnerability tests, etc.) and non-technical (policy/procedural, etc.) evaluations are occurring to continue to meet the regulatory security requirements and any changes in the environmental and operational that may affect sensitive (ePHI) data. To ensure that systems and networks are tested periodically to ensure that protections are still in place and working effectively.	Most Cisco systems and network devices included in the Healthcare Reference Model comply with generally accepted industry practices in the support of network and system testing and validation. Cisco routers and switches support SPAN and RSPAN for analyzing network traffic.
§164.312(a)(1)	Unique User Identification (a)(2)(i)	Ensure that each user who has access to sensitive (ePHI) data has a unique user id. Solution requires Identification controls.	Most Cisco applications, systems and devices support assigning unique user identifiers in support of this requirement. Unique Ids can be assigned to network users to access systems and applications and to network administrators to monitor and update the network infrastructure.

§164.312(a)(1)	Automatic Logoff (a)(2)(iii)	Ensure that policies, procedures and technical controls are in place to automatically logoff (terminate) a session after a predetermined period of inactivity.	Most Cisco applications, systems and devices support automatic logoff in support of this requirement. The time for session timeout can be configured based on policy requirements. Session timeout can vary by device or be configured for a universal timeout for all devices.
§164.312(d)	Person or Entity Authentication	Ensure that policies and procedures are in place to identify person or entity seeking access to sensitive (ePHI) data. Solution requires Authentication mechanisms.	Most Cisco applications, systems and devices support authentication in support of this requirement. Authentication can be Role-based authentication or Unique User Id accounts depending on the organizations policies, regulatory and business requirements.
§164.312(e)(1)	Integrity Controls (e)(2)(i)	Ensure that policies and procedures are in place to verify that data has not been altered or destroyed in an unauthorized manner during transmission. Solution requires signing of data or other integrity controls.	Cisco systems and devices use multiple forms of integrity monitoring to protect information from improper alteration or destruction of data at rest or in transit. Cisco devices support File-integrity monitoring or change- detection software on logs to ensure that existing log data cannot be changed without generating alerts. Integrity during transmission

4. Safeguard Mapping to Security Control Areas

In the remaining 15 Safeguard Areas in the current healthcare requirements, Verizon assessed the capability and capacity for Cisco's Healthcare Reference Model to support technically Direct Control that meet the intent of the Safeguard, or to provide Compensating Controls that, when implemented together in the Healthcare Reference Model, could support the fulfillment of the Safeguard; as a technology implementation that would in turn allow for a less complex operating procedure or management process to meet this Safeguard.

Verizon has identified the primary Physical, Network, System, and Application layer security controls that could be used to form a technical foundation of direct and compensating controls, for complying with the healthcare requirements. The breakdown of the remaining Safeguards into major control groups is as follows.

Control Group	Physical Security Controls	Network Security Controls	System Security Controls	Application Security Controls
PHY: Physical access, intrusion detection, and surveillance of users attempting to access or accessing physical network devices of systems containing or transporting ePHI. §164.310(a)(1) Access Control	• Electronic Access Controls • Intrusion Detection • Visual Surveillance			

IAM: Identification, Authentication, and Access Management controls for users and systems seeking access to ePHI across networks, systems, or applications. §164.308(a)(3)(i) Authorization and/or Supervision §164.308(a)(3)(i) Termination Procedures §164.308(a)(4)(i) Access Authorization §164.308(a)(4)(i) Access Est./ Modification	• Electronic Access Controls	• Network Access/ Authorization • Remote/ Wireless Access • Firewall/ • Segmentation • Encryption	• System Access/ • Authentication • Encryption • Backups	• Application Access/ Authentication • Logging/auditing • Encryption
LAM: Logging, Auditing, and Monitoring of users and systems attempting to access or accessing ePHI across networks, systems, or applications. §164.308(a)(1)(i) Information System Activity Review §164.308(a)(5)(i) Log-in Monitoring §164.308(a)(6)(i) Response and Reporting §164.312(b) Audit Controls	• Intrusion Detection • Visual Surveillance	• Network Access/ Authorization • Remote/ Wireless Access • Firewall Controls • Event Management • Activity Logging/Auditing • IDS/IPS	• System Access/ Authentication • Logging/Auditing • Encryption • IDS/IPS • Backups	• Application Access/ Authentication • Logging/auditing • Encryption

Control Group	Physical Security Controls	Network Security Controls	System Security Controls	Application Security Controls
E/D: Encryption/Decryption of data to protect ePHI while stored or in transit. §164.312(a)(1) Encryption / Decryption §164.312(c)(1) Data Integrity §164.312(e)(1) Encryption	•	• Network Layer Encryption	• System Layer Encryption	• Application Layer Encryption
EMO: Emergency Mode Operation control to allow granting of access to ePHI when need during emergency situations. §164.312(a)(2)(ii) Emergency Access	• Electronic Access Controls • Intrusion Detection • Visual Surveillance	• Network Access/ Authorization • Remote/ Wireless Access • Firewall • Segmentation • Event Management • Activity Logging/Auditing • IDS/IPS • Configuration Management	• System Access/ Authentication • Logging/Auditing • Encryption • IDS/IPS • Backups	• Application Access/ Authentication • Logging/auditing • Encryption

The table below provides a mapping of Safeguard into Physical, Network, System, and Application controls that, when used in combination, can fulfill the remaining 15 Safeguards and implementation of a low risk program to manage the protection of ePHI.

Type	Area	Citation	Title	Description	Direct Controls	Comp. Controls	Control Domain			
							Physical	Network	System	Application
	Security Management Process	§164.308(a)(1)(ii)(D)	Information System Activity Review	Implement procedures to regularly review records of information	Yes	Yes		Network, Remote, Wireless Access, network authentication,	Access Control, Authentication, Logging/Auditing	Access Control, Authentication, Logging/Auditing
	Workforce Security	§164.308(a)(3)(ii)(A)	Authorization and/or Supervision	Implement procedures for the authorization	Yes	Yes	Electronic Access	Network, Remote, Wireless Access,	Access Control, Authentication, Logging/Auditing	Access Control, Authentication, Logging/Auditing
		§164.308(a)(3)(i)(C)	Termination Procedures	Implement procedures to terminate access to ePHI upon	No	Yes	Electronic Access	Network, Remote, Wireless Access, network	Access Control, Authentication, Logging/Auditing	Access Control, Authentication, Logging/Auditing
	Information Access Management	§164.308(a)(4)(ii)(A)	Isolating Health Care Clearinghouse Functions	If a health care clearinghouse is part of a larger organization, the clearinghouse	Yes	Yes		Network, Remote, Wireless Access, network authentication,	Access Control, Authentication	
		§164.308(a)(4)(i)(B)	Access Authorization	Implement policies and procedures for granting access to ePHI (for example, through access to a workstation, Transaction, program, or other mechanism).	Yes	Yes	Electronic Access	Network, Remote, Wireless Access, network authentication, FW	Access Control, Authentication, Logging/Auditing	Access Control, Authentication, Logging/Auditing
		§164.308(a)(4)(i)(C)	Access Establishment and Modification	Implement policies and procedures that authorize access to ePHI and modify or delete access when it is no longer needed.	Yes	Yes	Electronic Access	Network, Remote, Wireless Access, network authentication, FW	Access Control, Authentication, Logging/Auditing	Access Control, Authentication, Logging/Auditing
	Awareness and Training	§164.308(a)(5)(ii)(C)	Log-in Monitoring	Implement procedures for monitoring log-in attempts to ePHI and report	Yes	Yes		Network, Remote, Wireless Access, network authentication,	Access Control, Authentication, Logging/Auditing	Access Control, Authentication, Logging/Auditing
	Incident Procedures	§164.308(a)(6)(ii)	Response and Reporting	Establish and implement policies and procedures for responding to suspected or	No	Yes	Intrusion Detection, Visual Surveillance	Network, Remote, Wireless Access, network authentication, Event Mgt.,	Access Control, Authentication, Logging/Auditing, IDS/IPS	
Administrative	Contingency Plan	§164.308(a)(7)(i)(C)	Emergency Mode Operations	Establish and implement procedures to enable continuation of critical business processed for the protection of the security of ePHI in emergency mode.	No	Yes	Electronic Access, Intrusion Detection, Visual Surveillance	Network, Remote, Wireless Access, network authentication, FW, Segmentation, Config. Mgt	Access Control, Authentication, Backups	

Physical	Facility Access Controls	§164.310(a)(2)(iii)	Access Control and Validation Procedures	Description: Implement procedures to control and validate a person's access to facilities based on their role or function and control access to software programs for testing and revision.	Yes	Yes	Electronic Access, Intrusion Detection, Visual Surveillance			
Technical	Access Controls	§164.312(a)(2)(ii)	Emergency Access Procedures	Description: Design and implement procedures for securely accessing ePHI in	Yes	Yes		Network, Remote, Wireless Access, network authentication, FW,	Access Control, Authentication, Backups	Access Control, Authentication, Logging/Auditing
		§164.312(a)(2)(iv)	Encryption and decryption	Description: Implement a mechanism to encrypt and	Yes	Yes		Firewall, Encryption	Encryption	
	Audit Controls	§164.312(b)	Audit Controls	Description: Ensure that there is a mechanism in place to record and examine activity in systems that contain or use	Yes	Yes		Network, Remote, Wireless Access, network authentication, FW, Segmentation, Event Mgt.,	Access Control, Authentication, Logging/Auditing Backups IDS/IPS	
	Integrity	§164.312(c)(1)	Integrity	Description: Implement policies and procedures to protect ePHI from improper alteration or	Yes	Yes		Encryption	Access Control, Authentication, Logging/Auditing Backups IDS/IPS	
	Transmission Security	§164.312(e)(2)(ii)	Encryption	Description: Implement a mechanism to encrypt ePHI whenever deemed appropriate.	Yes	Yes		Firewall, Encryption	Encryption	

5. Control Mapping to Cisco's Healthcare Reference Architecture

The applicability of Cisco's Reference Architecture to the healthcare requirements is shown as follows.

Domain Control	Control Description	Safeguards Assessed	Solution Components Reviewed
Physical Security Safeguards	Physical access, intrusion detection, and surveillance of users attempting to access or accessing physical network devices of systems containing or transporting ePHI	§164.308(a)(1)(i) Security Management Process §164.308(a)(3)(ii)(A) Authorization and/or Supervision §164.308(a)(4)(ii)(B) Access Authorization §164.308(a)(6)(ii) Response and Reporting §164.310(a)(1) Access Control	Cisco Physical Access Manager Cisco Physical Access Gateway

Administrative Safeguards	Supports access control at the network device level. Cisco devices have authentication on devices transiting the device and authentication on administrators configuring the device. IAM: Identification, Authentication, and Access Management controls for users and systems seeking access to ePHI across networks, systems, or applications. Supports access control at the System/Server levels. LAM: Logging, Auditing, and Monitoring of users and systems attempting to access or accessing ePHI across networks, systems, or applications.	§164.308(a)(1)(i) Security Management Process §164.308(a)(1)(ii)(D) Information System Activity Review §164.308(a)(3)(ii)(A) Authorization and/or Supervision §164.308(a)(3)(ii)(C) Termination Procedures §164.308(a)(4)(ii)(A) Isolating Health Care Clearinghouse Function §164.308(a)(4)(ii)(B) Access Authorization §164.308(a)(4)(ii)(C) Access Establishment and Modification §164.308(a)(5)(ii)(B) Protection from Malicious Software §164.308(a)(5)(ii)(C) Log-in Monitoring §164.308(a)(5)(ii)(D) Password Management §164.308(a)(6)(ii) Response and Reporting §164.308(a)(7)(i) Contingency Plan §164.308(a)(8) Evaluation	Server Vitalization—Servers - ISR SRE 900, UCS Express server ESXi Cisco Security Manager (CSM) Cisco Secure Access Control Server (ACS) Cisco Identity Services Engine (ISE) Ip Phone RSA Access Manager RSA Authentication Manager RSA Data Protection Manager RSA enVision HyTrust Cisco Prime Infrastructure VBlock—UCS - MDS - EMC SAN ASA Cisco Routers (ISR) Cisco Switches MDS Switch Fabric Cisco Wireless Cisco Security devices

Technical Safeguards	Supports independent protection of EPHI while at rest and in transit. E/D Common controls to protect data, independent of network or system layer. IAM: Identification, Authentication, and Access Management controls for users and systems seeking access to ePHI across networks, systems, or applications. Supports access control at the System/Server levels. Supports identifying anomalous activity in advance of more serious issues, and incident response. Supports data integrity and emergency operations	164.312(a)(2)(i) Unique User Identification 164.312(a)(2)(ii) Emergency Access Procedures 164.312(a)(2)(iii) Automatic Logoff 164.312(a)(2)(iv) Encryption and Decryption 164.312(b) Audit Controls 164.312(c)(1) Data Integrity 164.312(d) Person or Entity Authentication 164.312(e)(2)(i) Transmission Integrity Controls 164.312(e)(2)(ii) Transmission Encryption	Server Vitalization—Servers - ISR SRE 900, UCS Express server ESXi Cisco Security Manager (CSM) Cisco Secure Access Control Server (ACS) Cisco Identity Services Engine (ISE) Ip Phone RSA Access Manager RSA Authentication Manager RSA Data Protection Manager RSA enVision HyTrust Cisco Prime Infrastructure VBlock—UCS - MDS - EMC SAN ASA Cisco Routers (ISR) Cisco Switches MDS Switch Fabric Cisco Wireless Cisco Security devices

6. Application of the Healthcare Reference Architecture

Cisco's Healthcare Reference architecture provides a robust networking core and infrastructure that can support a Customer's implementation of network security controls and system security controls as part of their security program and as required HIPAA-Required Risk Management process.

The architecture also provides both strong common security controls through network devices and security control and management systems that are highly Capable to support data security, and specific security management components that are directly Applicable to meet HIPAA safeguard' control requirements. Strong common controls include:

- Protection from Malicious Software (§164.308(a)(5)(i)).
- Password Management (§164.308(a)(5)(i))
- Periodic Technical and Non-Technical Evaluation (§164.312(a)(1))
- Unique User Identification (§164.312(a)(1))

- Automatic Logoff (§164.312(a)(1))
- Person or Entity Authentication (§164.312(d))
- Integrity Controls (§164.312(e)(1))

The fact that Cisco devices universally support the core security controls outlined in HIPAA safeguards, allows a customer to implement the reference architecture with the confidence that their resulting infrastructure will support HIPAA compliance from the outset, and with the knowledge that any additional use of Cisco's security management tools, will only enhance the protection of ePHI and further support Healthcare compliance.

Cisco's Healthcare Reference Architecture also provides directly applicable security control features and capabilities owing to the depth of security management tools provided in this model. Directly Applicable control include:

- **Physical Access Control, Intrusion Detection, and Visual Surveillance.** Cisco's Physical Access Manager and Physical Access Gateway products provide the control structure for to use electronic access controls, intrusion detection, and visual surveillance components to control physical access to a wide range of healthcare facilities from landlord closets housing Clinic IT equipment in leasing situations, to the control of physical security at remote and co-located Clinics, to the development and integration of remote facilities into Hospital physical security systems.
- **Network Access and Authentication Controls for wired, wireless, and remote Networks**. Cisco's Reference architecture provides for network access control and authentication of both users and systems operating on wired WAN/LANs, access wireless networks, and access Customer networks remotely, in a seamless approach that supports multiple HIPAA safeguard requirements for Identify Management, Access Controls, user and system authorization, and authentication.
- **Network Segmentation, Segregation, and Isolation Capabilities**. Cisco's healthcare reference architecture provide unsurpassed capability to deliver fine grained control over the ability of a user on a clinical or administrative workstation, on a medical device, or administrative console to have network access to systems, servers, and storage devices that contain ePHI. Cisco's architecture allow a Customer to develop and maintain segmentation between administrative and clinical systems, to structure sub-networks for only administrative workstations, medical devices, server farms, and publicly-facing web servers. Customers can establish and maintain user and system segregation by their role/function within Clinics and Hospitals, and Customers can demonstrate isolation of EPHI-containing systems/storage as a part of their overall ePHI protection strategy. Customer can meet HIPAA's clearinghouse isolation requirements. Customers can plan for and execute emergency rerouting and access strategies to support continued operations during natural disasters, in order to maintain patient data security while support emergency care. Customers can ensure that workforce members are granted access based on their role in the institution, and can also terminate access at the network level to support HIPAA's Sanction/Termination requirements.
- **Logging, Auditing, and Monitoring Capabilities**. Cisco's Healthcare Reference Architecture also provides robust and well managed logging capabilities, support routine and event-driven authoring, support continuous monitoring of the network and system environment for control, and provides the ability to investigate and interrogate devices as needed in support of data breach events. The Reference Architecture supports HIPAA's Information System Activity Review requirements by providing an infrastructure to log, audit, and monitor network and system behavior and support the tracking of user and system access or patient information. While used as part of a total activity review strategy, Cisco's Security Manager, Identity Service Engine, and Suite of RSA products, for a solid platform for developing a total activity review and control solution. Cisco' Reference Architecture provide the centralized logging capabilities and auditing features to support effective audit of ePHI controls by Customer's security team, internal auditors, external auditors, and regulators. Cisco's suite of IDS/IPS products in the Reference Architecture provide the Customer with ab alerting foundation to support the "Response and Reporting" Safeguard requirements.

- **Encryption of ePHI**. Cisco's reference architecture allows Customers to realize the substantial security control that can be exerted through ePHI encryption while at rest and in transit to further protect ePHI when application layer security control might fail or be bypassed, or when operational errors inadvertently release patient information or lose track of servers containing ePHI. The reference architecture core and vBlock products support seamless data encryption and decryption on the fly, without the traditional performance concerns. The reference architecture also support HIPAA's data integrity requirements, protecting ePHI from "improper alteration" while stored or while in transit across private and public networks.

7. Appendix

Healthcare Security Requirements

Standards	Sections	Implementation Specifications R=Required, (A)=Addressable	Type
Security Standards: General Rules			
Security Standards: General Rules	§164.306	Security Standards General Rules	R
Administrative Safeguards			
Security Management Process	§164.308(a)(1)	Security Management Process	R
	§164.308(a)(1)(ii)(A)	Risk Analysis	R
	§164.308(a)(1)(ii)(B)	Risk Management	R
	§164.308(a)(1)(ii)(C)	Sanction Policy	R
	§164.308(a)(1)(ii)(D)	Information System Activity Review	R
Assigned Security Responsibility	§164.308(a)(2)	Assigned Security Responsibility	R
Workforce Security	§164.308(a)(3)(i)	Workforce Security	R
	§164.308(a)(3)(i)(A)	Authorization and/or Supervision	A
	§164.308(a)(3)(i)(B)	Workforce Clearance Procedures	A
	§164.308(a)(3)(i)(C)	Termination Procedures	A
Information Access Management	§164.308(a)(4)(i)	Information Access Management	R
	§164.308(a)(4)(i)(A)	Isolating Healthcare Clearinghouse Functions	R
	§164.308(a)(4)(i)(B)	Access Authorization	A
	§164.308(a)(4)(i)(C)	Access Establishment and Modification	A
Security Awareness and Training	§164.308(a)(5)(i)	Security Awareness and Training	R
	§164.308(a)(5)(i)(A)	Security Reminders	A
	§164.308(a)(5)(i)(B)	Protection from Malicious Software	A
	§164.308(a)(5)(i)(C)	Log-in Monitoring	A
	§164.308(a)(5)(i)(D)	Password Management	A

Security Incident Procedures	§164.308(a)(6)(i)	Security Incident Procedures	R
	§164.308(a)(6)(ii)	Response and Reporting	R
Contingency Planning	§164.308(a)(7)(i)	Contingency Plan	R
	§164.308(a)(7)(i)(A)	Data Backup Plan	R
	§164.308(a)(7)(i)(B)	Disaster Recovery Plan	R
	§164.308(a)(7)(i)(C)	Emergency Mode Operation Plan	R
	§164.308(a)(7)(i)(D)	Testing and Revision Procedures	A
	§164.308(a)(7)(i)(E)	Applications and Data Criticality Analysis	A
Evaluation	§164.308(a)(8)	Evaluation	R
BA Contracts and Other Arrangements	§164.308(b)(1)	BA Contracts and other arrangements	R
	§164.308(b)(2)	BA Exceptions	R
	§164.308(b)(3)	Satisfactory Assurances under b2	R
	§164.308(b)(4)	Satisfactory Assurances under b1	R
Physical Safeguards			
Facility Access Controls	§164.310(a)(1)	Facility Access Controls	R
	§164.310(a)(2)(i)	Contingency Operations	A
	§164.310(a)(2)(ii)	Facility Security Plan	A
	§164.310(a)(2)(iii)	Access Control and Validation Procedures	A
	§164.310(a)(2)(iv)	Maintenance Records	A
Workstation Use	§164.310(b)	Workstation Use	R
Workstation Security	§164.310(c)	Workstation Security	R
Device and Media Controls	§164.310(d)(1)	Device and Media Controls	R
	§164.310(d)(2)(i)	Disposal	R
	§164.310(d)(2)(ii)	Media Re-use	R
	§164.310(d)(2)(ii)	Accountability	A
	§164.310(d)(2)(iv)	Data Backup and Storage	A
Technical Safeguards			
Access Control	§164.312(a)(1)	Access Control	R
	§164.312(a)(2)(i)	Unique User Identification	R
	§164.312(a)(2)(ii)	Emergency Access Procedure	R
	§164.312(a)(2)(iii)	Automatic Logoff	A
	§164.312(a)(2)(iv)	Encryption and Decryption	A
Audit Controls	§164.312(b)	Audit Controls	R
Integrity	§164.312(c)(1)	Integrity	R
	§164.312(c)(2)	Mechanism to Authenticate Electronic Protected Health Information	A
Authentication	§164.312(d)	Person or Entity Authentication	R

Transmission Security	§164.312(e)(1)	Transmission Security	R
	§164.312(e)(2)(i)	Integrity Controls	A
	§164.312(e)(2)(ii)	Encryption	A
Organizational Requirements			
BA Contracts and Other Arrangements	§164.314(a)(1)(i)	Business Associate Contracts and Other Arrangements	R
	§164.314(a)(2)(i)(A)	Business Associate Compliance	R
	§164.314(a)(2)(i)(B)	BA Subcontractor Compliance	R
	§164.314(a)(2)(i)(C)	BA Security Incident Reporting	R
	§164.314(a)(2)(ii)	Other Arrangements	R
	§164.314(a)(2)(iii)	Other Arrangements Subcontractor Compliance	R
Requirements for Group Health Plans	§164.314(b)(1)	Requirements for Group Health Plans	R
	§164.314(b)(2)(i)	BA Information Security Controls	R
	§164.314(b)(2)(ii)	Separation of GHP and sponsor	R
	§164.314(b)(2)(iii)	Ensure Agents implement security	R
	§164.314(b)(2)(iv)	Report incidents to group health plan	R
Policies and Procedures and Documentation Requirements			
Policies and Procedures and Documentation Requirements	§164.316(a)	Maintaining Policy and Procedures	R
	§164.316(b)(1)(i)	Written Policy and Procedures	R
	§164.316(b)(1)(ii)	Written Record of Risk Management	R
	§164.316(b)(2)(i)	Documentation Time Limit	R
	§164.316(b)(2)(ii)	Documentation Availability	R
	§164.316(b)(2)(iii)	Documentation Updates	R

List of Interviews

The following members of the Cisco Architecture Team were interviewed as part of the PCI Assessment. The results from the PCI Assessment were used as a direct reference for the HIPAA Assessment.

Interviewee(s)	Title
Christian Janoff, Bart McGlothin	Network architecture, firewalls, routers, switches, wireless, IDS/IPS, Audit Logging, Access Control / Authentication, CSM, Wireless, LMS, Cisco Virtual Service Gateway, ASA
Sai Balabhadrapatruni	ASA, Cisco IPS
Jamey Heary	Cisco ISE
Raju Satyan	Cisco Prime LMS with Pari Compliance Module
Tom Hua	CSM
Sheri Spence	EMC SAN
Syed Ghayur	Nexus 1kv
Mike Adler, Sujit Ghosh	Wireless lab
K. Sigel, R. Budko	HyTrust

Syed Ghayur	Cisco Virtual Service Gateway
Pandit Panburana, Mourad Cherfaoui	CUCM
Rupesh Chakkingal, David Valiquette	RSA Data Protection Manager
Danny Dhillon	RSA enVision, RSA Authentication Manager, RSA Data Protection Manager, RSA Access Manager, RSA Authentication Manager

List of Documents

The following documents were reviewed as part of the PCI Assessment. The results of the PCI Assessment were used as a direct reference for the HIPAA Assessment.

Document	Date
Enterprise Retail PCI DSS 2.0 pdf	11/17/2010
Switch and router configs	4/15/2011
Switch configs - branches	4/15/2011
Common requirements questions across all devices.xls	12/01/2010
Products Alignment_2010-10-13.xlsx	10/13/2010
PCI Retail Solution Products.xlsx	04/15/2011
ASA, router, ACE Load Balancer, and IPS configurations	11/12/2012
Compliance_LAB_Diagram_2012-12-03 - Internet Edge Page.pdf	12/06/2012
20121130 PCI DSS and IPv6.docx	11/30/2012
LMS and Pari_DIG Revision_2012-11-11.docx	11/12/2012
Lab_IP_Addressing_and_Consoles.xlsx	11/12/2012
Cisco ISE at a glance	11/30/2012
Cisco ISE Data Sheet	11/30/2012

APPENDIX D

Simplified Crosswalk—HIPAA, PCI, and SOX

Title	Citation	PCI Cross Reference	SOX Cross Reference
Security Management Process	164.308(a)(1)(i)	12.1, 12.1.1, 12.1.1, 12.1.3, 12.2, 12.6, 12.9, 12.9.1, 12.9.2, 12.9.3, 12.9.4 NA - ALL	CA (DS5) Monitoring CE (ME12) Internal Control Program
Risk Analysis	164.308(a)(1)(ii)(A)		CA (A16) Risk Assessment
Risk Management	164.308(a)(1)(ii)(B)		CA (A16) Risk Assessment
Information System Activity Review	164.308(a)(1)(ii)(D)	**10.2.7** (Y), 10.3, **10.3.1** (Y), **10.3.2** (Y), **10.3.3** (Y), **10.3.4** (Y), **10.3.5** (Y), **10.3.6** (Y), 10.6, 11.5, 12.9.6,	CA (DS5) Monitoring
Assigned Security Responsibility	164.308(a)(2)		CA (DS5) Monitoring
Authorization and/or Supervision	164.308(a)(3)(ii)(A)	2.2.3, **7.1.4** (Y), 7.2, **7.2.3** (Y), **8.2** (Y), 8.5.1, 8.5.16, **10.2.7** (Y), 10.3, **10.3.1** (Y), **10.3.2** (Y), **10.3.3** (Y), **10.3.4** (Y), **10.3.5** (Y), **10.3.6** (Y), 10.6, 11.5,	
Termination Procedures	164.308(a)(3)(ii)(C)	**8.2** (Y), 8.5.1, 8.5.16,	
Isolating Health Care Clearinghouse Function	164.308(a)(4)(ii)(A)	2.1.1, 2.2.3, 6.6, **7.1.4** (Y), 12.8.2,	
Access Authorization	164.308(a)(4)(ii)(B)	2.2.3, **7.1.4** (Y), 7.2, **7.2.3** (Y), **8.2** (Y), 8.5.1, 8.5.16,	
Access Establishment and Modification	164.308(a)(4)(ii)(C)	**8.2** (Y), 8.5.1, 8.5.16,	
Protection from Malicious Software	164.308(a)(5)(ii)(B)	5.1, 5.1.1, 5.2, NA - ALL	CA (DS9) Manage Configuration

Log-in Monitoring	164.308(a)(5)(ii)(C)	**10.1** (Y), 10.2, **10.2.1** (Y), **10.2.5** (Y), **10.2.7** (Y), 10.3, **10.3.1** (Y), **10.3.2** (Y), **10.3.3** (Y), **10.3.4** (Y), **10.3.5** (Y), **10.3.6** (Y), **10.5.4** (Y), 10.6, 11.5,	CA (DS5) Monitoring
Password Management	164.308(a)(5)(ii)(D)	2.1, 2.1.1, **8.4** (Y), 8.5, 8.5.2, 8.5.3, 8.5.7, **8.5.8** (Y), **8.5.9** (Y), **8.5.10** (Y), **8.5.11** (Y), **8.5.12** (Y), **8.5.13** (Y), **8.5.14** (Y),	
Response and Reporting	164.308(a)(6)(ii)	12.6, 12.9, 12.9.1, 12.9.2, 12.9.3, 12.9.4, 12.9.6, NA-ALL	CA (DS5) Monitoring
Contingency Plan	164.308(a)(7)(i)	9.1.1 NA	
Evaluation	164.308(a)(8)	11.3, 12.1, 12.1.1, 12.1.2, 12.1.3, 12.2 NA-ALL	CA (DS5) Monitoring
Facility Access Control and Validation Procedures	164.310(a)(2)(iii)	NA	CA (DS12) Physical Security
Unique User Identification	164.312(a)(2)(i)	3.2, **8.1** (Y), **8.2** (Y), 8.5.1, **8.5.8** (Y), 8.5.16, 12.3.2	
Emergency Access Procedure	164.312(a)(2)(ii)	**7.1.4** (Y)	
Automatic Logoff	164.312(a)(2)(iii)	**8.5.15** (Y), 12.3.8	
Encryption and Decryption	164.312(a)(2)(iv)	3.5, 3.5.1, 3.5.2, 3.6, 3.6.1, 3.6.2, 3.6.3, 3.6.4, 3.6.5, 3.6.6, 3.6.7, 3.6.8, NA -ALL	
Audit Controls	164.312(b)	**10.1** (Y), 10.2, **10.2.1** (Y), **10.2.5** (Y), **10.2.7** (Y), 10.3, **10.3.1** (Y), **10.3.2** (Y), **10.3.3** (Y), **10.3.4** (Y), **10.3.5** (Y), **10.3.6** (Y), **10.5.4** (Y), 10.6, 11.5,	
Data Integrity	164.312(c)(1)	2.3, **4.1** (Y), 4.1.1 (Y),	CA (DS9) Manage Configuration
Person or Entity Authentication	164.312(d)	3.2, **8.1** (Y), **8.2** (Y), 8.5.1 , **8.5.8** (Y), 8.5.16, 12.3.2,	
Integrity Controls	164.312(e)(2)(i)	2.1.1, **4.1** Y, 4.1.1	
Encryption	164.312(e)(2)(ii)	2.1.1, **4.1** Y, 4.1.1	

APPENDIX E

Detailed Full Running Configurations

Table of Contents

Data Center 1
- WAN 1
  - ASA-WAN-1 1
  - ASA-WAN-1_IDS 11
  - RWAN-1 13
  - RWAN-2 19
  - SWAN-1 24
  - SWAN-3 28
- Core 33
  - RCORE-1 33
  - RCORE-2 42
- Aggregation 51
  - ASA-DC-1 51
  - RAGG-1-RUNNING 63
  - RAGG-1-VDC1-RUNNING 68
  - RAGG-1-VDC2-RUNNING 72
  - RAGG-2-RUNNING 84
  - RAGG-2-VDC1-RUNNING 89
  - RAGG-2-VDC2-RUNNING 93
  - N1KV-1-RUNNING 104
  - VSG-TENANT-1-RUNNING 109
  - RSERV-1 111
  - RSERV-2 121
- Access 131

SACCESS-1 131
SACCESS-2 140
SACCESS-3 148
SACCESS-4 157
SACCESS-5 165
Storage 172
MDS-DC-1-RUNNING 172
MDS-DC-2-RUNNING 185
Internet Edge 195
WAN 195
RIE-1 195
RIE-2 204
Converged Core/Aggregation 211
ASA-IE-1 211
DMZ-IDS-1 223
DMZ-ASASM 225
DMZ-ACE-1 237
DMZ-ACE-1_ECOM 239
RIE-3 241
Branch 250
Large Branch 250
R-A2-LRG-1 250
R-A2-LRG-2 283
S-A2-LRG-1 316
S-A2-LRG-2 326
S-A2-LRG-3 333
S-A2-LRG-4 345
S-A2-LRG-5 358
Medium Branch 362
R-A2-MED-1 362
R-A2-MED-2 396
S-A2-MED-1 430
S-A2-MED-3 440
Small Branch 444
R-A2-SMALL 444
S-A2-SMALL 475
Mini Branch 486
R-A2-MINI-1 486
S-A2-MINI-1 518
S-A2-MINI-2 522

Convenience 526
R-A2-CONV-1 526
S-A2-CONV-1 558
Managed Service Provider 562
FW-A2-MSP-1 562
S-A2-MSP-1 579

Data Center

WAN

ASA-WAN-1

```
ASA Version 9.1(1)
!
firewall transparent
terminal width 511
hostname ASA-WAN-1
domain-name cisco-irn.com
enable password <removed>
passwd <removed>
names
!
interface GigabitEthernet0/0
 nameif outside
 bridge-group 1
 security-level 0
!
interface GigabitEthernet0/1
 nameif inside
 bridge-group 1
 security-level 100
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
!
interface GigabitEthernet0/3
 description LAN/STATE Failover Interface
!
interface GigabitEthernet0/4
 shutdown
 no nameif
 no security-level
!
interface GigabitEthernet0/5
 shutdown
 no nameif
 no security-level
!
interface GigabitEthernet0/6
 shutdown
 no nameif
```

```
 no security-level
!
interface GigabitEthernet0/7
 shutdown
 no nameif
 no security-level
!
interface Management0/0
 management-only
 no nameif
 no security-level
!
interface BVI1
 ip address 192.168.11.20 255.255.255.0 standby 192.168.11.21
!
boot system disk0:/asa911-smp-k8.bin
ftp mode passive
clock timezone PST -8
clock summer-time PDT recurring
dns server-group DefaultDNS
 domain-name cisco-irn.com
object network AdminStation
 host 192.168.41.101
object network AdminStation2
 host 192.168.41.102
object network AdminStation4-bart
 host 10.19.151.99
object network EMC-NCM
 host 192.168.42.122
 description EMC Network Configuration Manager
object network CSManager
 host 192.168.42.133
 description Cisco Security Manager
object network AdminStation3
 host 192.168.42.138
object network ActiveDirectory.cisco-irn.com
 host 192.168.42.130
object network Branches-ALL
 subnet 10.10.0.0 255.255.0.0
 description all branch networks
object network vSphere-1
 host 192.168.41.102
 description vSphere server for Lab
object network WCSManager
 host 192.168.43.135
 description Wireless Manager
object network PAME-DC-1
 host 192.168.44.111
object network MSP-DC-1
 host 192.168.44.121
 description Data Center VSOM
object network DC-ALL
 subnet 192.168.0.0 255.255.0.0
 description All of the Data Center
object network RSA-enVision
 host 192.168.42.124
 description RSA EnVision Syslog collector and SIM
object network TACACS
 host 192.168.42.131
 description Csico Secure ACS server for TACACS and Radius
object network RSA-AM
 host 192.168.42.137
 description RSA Authentication Manager for SecureID
object network ISE-2
```

```
 host 192.168.42.112
 description HA ISE Server
object network ISE-1
 host 192.168.42.111
 description ISE server for NAC
object network MS-Update
 host 192.168.42.150
 description Windows Update Server
object network MSExchange
 host 192.168.42.140
 description Mail Server
object network DC-POS
 subnet 192.168.52.0 255.255.255.0
 description POS in the Data Center
object service RPC
 service tcp destination eq 135
object service LDAP-GC
 service tcp destination eq 3268
object service LDAP-GC-SSL
 service tcp destination eq 3269
object service Kerberos-TCP
 service tcp destination eq 88
object service Microsoft-DS-SMB
 service tcp destination eq 445
 description Microsoft-DS Active Directory, Windows shares Microsoft-DS SMB file sharing
object service LDAP-UDP
 service udp destination eq 389
object service RPC-HighPorts
 service tcp destination range 1024 65535
object service IP-Protocol-97
 service 97
 description IP protocol 97
object service TCP1080
 service tcp destination eq 1080
object service TCP8080
 service tcp destination eq 8080
object service RDP
 service tcp destination eq 3389
 description Windows Remote Desktop
object network LMS
 host 192.168.42.139
 description Cisco Prime LMS
object-group network BRANCH-POS
 network-object 10.10.0.0 255.255.0.0
object-group network Admin-Systems
 network-object object EMC-NCM
 network-object object AdminStation
 network-object object AdminStation2
 network-object object CSManager
 network-object object AdminStation3
 network-object object ISE-1
 network-object object ISE-2
 network-object object LMS
object-group network DC-Wifi-Controllers
 description Central Wireless Controllers for branchs
 network-object 192.168.43.21 255.255.255.255
 network-object 192.168.43.22 255.255.255.255
object-group network DC-Wifi-MSE
 description Mobility Service Engines
 network-object 192.168.43.31 255.255.255.255
 network-object 192.168.43.32 255.255.255.255
object-group network DM_INLINE_NETWORK_5
 network-object object ISE-1
 network-object object ISE-2
```

```
 network-object object RSA-AM
 network-object object TACACS
object-group network DM_INLINE_NETWORK_6
 network-object object ISE-1
 network-object object ISE-2
object-group network DC-WAAS
 description WAE Appliances in Data Center
 network-object 192.168.48.10 255.255.255.255
 network-object 192.168.49.10 255.255.255.255
 network-object 192.168.47.11 255.255.255.255
 network-object 192.168.47.12 255.255.255.255
object-group network NTP-Servers
 description NTP Servers
 network-object 192.168.62.161 255.255.255.255
 network-object 162.168.62.162 255.255.255.255
object-group icmp-type DM_INLINE_ICMP_1
 icmp-object echo
 icmp-object echo-reply
 icmp-object time-exceeded
 icmp-object traceroute
 icmp-object unreachable
object-group service DM_INLINE_TCP_3 tcp
 port-object eq www
 port-object eq https
object-group network DC-POS-Tomax
 description Tomax POS Communication from Store to Data Center
 network-object 192.168.52.96 255.255.255.224
object-group network DC-POS-SAP
 description SAP POS Communication from Store to Data Center
 network-object 192.168.52.144 255.255.255.240
object-group network DC-POS-Oracle
 description Oracle POS Communication from Store to Data Center
 network-object 192.168.52.128 255.255.255.240
object-group service HTTPS-8443
 service-object tcp destination eq 8443
object-group network DM_INLINE_NETWORK_7
 network-object object MSP-DC-1
 network-object object PAME-DC-1
object-group service DNS-Resolving
 description Domain Name Server
 service-object tcp destination eq domain
 service-object udp destination eq domain
object-group network DM_INLINE_NETWORK_8
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
object-group service vCenter-to-ESX4
 description Communication from vCetner to ESX hosts
 service-object tcp destination eq 5989
 service-object tcp destination eq 8000
 service-object tcp destination eq 902
 service-object tcp destination eq 903
object-group network DM_INLINE_NETWORK_9
 network-object object DC-POS
 group-object DC-POS-Oracle
 group-object DC-POS-SAP
 group-object DC-POS-Tomax
object-group service TFTP
 description Trivial File Transfer
 service-object tcp destination eq 69
 service-object udp destination eq tftp
object-group service LWAPP
 description LWAPP UDP ports 12222 and 12223
 service-object udp destination eq 12222
 service-object udp destination eq 12223
```

```
object-group service CAPWAP
 description CAPWAP UDP ports 5246 and 5247
 service-object udp destination eq 5246
 service-object udp destination eq 5247
object-group service DM_INLINE_SERVICE_10
 group-object HTTPS-8443
 service-object tcp destination eq www
 service-object tcp destination eq https
object-group service ESX-SLP
 description CIM Service Location Protocol (SLP) for VMware systems
 service-object udp destination eq 427
 service-object tcp destination eq 427
object-group service DM_INLINE_SERVICE_11
 group-object ESX-SLP
 service-object tcp destination eq www
 service-object tcp destination eq https
 service-object tcp destination eq ssh
 group-object vCenter-to-ESX4
object-group service CISCO-WAAS
 description Ports for Cisco WAAS
 service-object tcp destination eq 4050
object-group service Netbios
 description Netbios Servers
 service-object udp destination eq netbios-dgm
 service-object udp destination eq netbios-ns
 service-object tcp destination eq netbios-ssn
object-group service Cisco-Mobility
 description Mobility ports for Wireless
 service-object udp destination eq 16666
 service-object udp destination eq 16667
object-group service DM_INLINE_SERVICE_12
 group-object CAPWAP
 group-object Cisco-Mobility
 service-object object IP-Protocol-97
 group-object LWAPP
 service-object tcp destination eq https
 service-object udp destination eq isakmp
object-group service DM_INLINE_SERVICE_13
 service-object tcp-udp destination eq sip
 service-object tcp destination eq 2000
object-group network DM_INLINE_NETWORK_2
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
 network-object object WCSManager
object-group network DM_INLINE_NETWORK_3
 network-object object DC-ALL
 group-object BRANCH-POS
object-group network DM_INLINE_NETWORK_4
 network-object object MSP-DC-1
 network-object object PAME-DC-1
object-group service DM_INLINE_SERVICE_2
 service-object icmp
 group-object HTTPS-8443
 service-object tcp destination eq https
 service-object tcp destination eq ssh
 service-object udp destination eq snmp
object-group service DM_INLINE_SERVICE_3
 group-object DNS-Resolving
 service-object object Kerberos-TCP
 service-object object LDAP-GC
 service-object object LDAP-GC-SSL
 service-object object LDAP-UDP
 service-object object Microsoft-DS-SMB
 service-object object RPC
```

```
 service-object object RPC-HighPorts
 service-object tcp destination eq ldap
 service-object tcp destination eq ldaps
 service-object udp destination eq 88
 service-object udp destination eq netbios-dgm
 service-object udp destination eq ntp
object-group service DM_INLINE_SERVICE_4
 service-object tcp destination eq https
 service-object tcp destination eq ssh
 group-object vCenter-to-ESX4
object-group service DM_INLINE_SERVICE_5
 group-object CAPWAP
 service-object object IP-Protocol-97
 group-object LWAPP
 group-object TFTP
 service-object tcp destination eq www
 service-object tcp destination eq https
 service-object tcp destination eq ssh
 service-object tcp destination eq telnet
 service-object udp destination eq isakmp
object-group service DM_INLINE_SERVICE_6
 group-object HTTPS-8443
 service-object object RDP
 service-object object TCP1080
 service-object object TCP8080
 service-object icmp echo
 service-object icmp echo-reply
 service-object tcp destination eq ftp
 service-object tcp destination eq www
 service-object tcp destination eq https
 service-object tcp destination eq ssh
object-group service DM_INLINE_SERVICE_7
 group-object CISCO-WAAS
 group-object HTTPS-8443
 service-object object Microsoft-DS-SMB
 group-object Netbios
object-group service DM_INLINE_SERVICE_8
 service-object tcp-udp destination eq sip
 service-object tcp destination eq 2000
object-group service DM_INLINE_SERVICE_14
 group-object CISCO-WAAS
 group-object HTTPS-8443
 service-object object Microsoft-DS-SMB
 group-object Netbios
object-group service DM_INLINE_SERVICE_15
 group-object DNS-Resolving
 service-object object Kerberos-TCP
 service-object object LDAP-GC
 service-object object LDAP-GC-SSL
 service-object object LDAP-UDP
 service-object object Microsoft-DS-SMB
 service-object object RPC
 service-object object RPC-HighPorts
 service-object tcp destination eq ldap
 service-object tcp destination eq ldaps
 service-object udp destination eq 88
 service-object udp destination eq netbios-dgm
 service-object udp destination eq ntp
object-group service DM_INLINE_SERVICE_9
 service-object tcp destination eq ldap
 service-object tcp destination eq ldaps
 service-object udp destination eq domain
object-group service DM_INLINE_TCP_1 tcp
 port-object eq www
```

```
 port-object eq https
object-group service DM_INLINE_TCP_2 tcp
 port-object eq www
 port-object eq https
 port-object eq imap4
 port-object eq pop3
 port-object eq smtp
object-group service DM_INLINE_UDP_1 udp
 port-object eq snmp
 port-object eq snmptrap
 port-object eq syslog
object-group service DM_INLINE_UDP_2 udp
 port-object eq 1812
 port-object eq 1813
access-list INSIDE extended permit ip any any
access-list INSIDE extended permit object-group DM_INLINE_SERVICE_2 object-group
Admin-Systems object-group DM_INLINE_NETWORK_3
access-list INSIDE remark Allow Active Directory Domain
access-list INSIDE extended permit object-group DM_INLINE_SERVICE_3 object
ActiveDirectory.cisco-irn.com object Branches-ALL
access-list INSIDE remark VMWare - ESX systems
access-list INSIDE extended permit object-group DM_INLINE_SERVICE_4 object vSphere-1
object Branches-ALL
access-list INSIDE remark Wireless Management to Stores
access-list INSIDE extended permit object-group DM_INLINE_SERVICE_5 object-group
DM_INLINE_NETWORK_2 object Branches-ALL
access-list INSIDE remark Physical security systems
access-list INSIDE extended permit tcp object-group DM_INLINE_NETWORK_4 object
Branches-ALL eq https
access-list INSIDE remark Allow Management of branch systems
access-list INSIDE extended permit object-group DM_INLINE_SERVICE_6 object DC-ALL object
Branches-ALL
access-list INSIDE remark WAAS systems
access-list INSIDE extended permit object-group DM_INLINE_SERVICE_7 object-group DC-WAAS
object Branches-ALL
access-list INSIDE remark Voice calls
access-list INSIDE extended permit object-group DM_INLINE_SERVICE_8 object DC-ALL object
Branches-ALL
access-list INSIDE remark Drop and Log all other traffic
access-list INSIDE extended deny ip any any log
access-list OUTSIDE extended permit ip any any
access-list OUTSIDE remark Connectivity validation
access-list OUTSIDE extended permit icmp object Branches-ALL any object-group
DM_INLINE_ICMP_1
access-list OUTSIDE remark Internet Browsing
access-list OUTSIDE extended permit tcp object Branches-ALL any object-group
DM_INLINE_TCP_3
access-list OUTSIDE remark Config uploading
access-list OUTSIDE extended permit tcp object Branches-ALL object EMC-NCM eq ssh
access-list OUTSIDE remark Log reporting
access-list OUTSIDE extended permit udp object Branches-ALL object RSA-enVision
object-group DM_INLINE_UDP_1
access-list OUTSIDE remark Authentication and DNS lookup
access-list OUTSIDE extended permit object-group DM_INLINE_SERVICE_9 object Branches-ALL
object ActiveDirectory.cisco-irn.com
access-list OUTSIDE remark Authentication and authorization
access-list OUTSIDE extended permit tcp object Branches-ALL object TACACS eq tacacs
access-list OUTSIDE remark Time Sync
access-list OUTSIDE extended permit udp object Branches-ALL object-group NTP-Servers eq
ntp
access-list OUTSIDE remark Authentication
access-list OUTSIDE extended permit udp object Branches-ALL object-group
DM_INLINE_NETWORK_5 object-group DM_INLINE_UDP_2
access-list OUTSIDE remark Authentication web portal
```

```
access-list OUTSIDE extended permit object-group DM_INLINE_SERVICE_10 object Branches-ALL
object-group DM_INLINE_NETWORK_6
access-list OUTSIDE remark VMWare ESX to Data Center
access-list OUTSIDE extended permit object-group DM_INLINE_SERVICE_11 object Branches-ALL
object vSphere-1
access-list OUTSIDE remark Physical security systems
access-list OUTSIDE extended permit tcp object Branches-ALL object-group
DM_INLINE_NETWORK_7 eq https
access-list OUTSIDE remark Wireless control systems
access-list OUTSIDE extended permit object-group DM_INLINE_SERVICE_12 object Branches-ALL
object-group DM_INLINE_NETWORK_8
access-list OUTSIDE remark Voice calls
access-list OUTSIDE extended permit object-group DM_INLINE_SERVICE_13 object Branches-ALL
object DC-ALL
access-list OUTSIDE remark WAAS systems
access-list OUTSIDE extended permit object-group DM_INLINE_SERVICE_14 object Branches-ALL
object-group DC-WAAS
access-list OUTSIDE remark Allow Active Directory Domain
access-list OUTSIDE extended permit object-group DM_INLINE_SERVICE_15 object Branches-ALL
object ActiveDirectory.cisco-irn.com
access-list OUTSIDE remark Allow Windows Updates
access-list OUTSIDE extended permit tcp object Branches-ALL object MS-Update object-group
DM_INLINE_TCP_1
access-list OUTSIDE remark Allow Mail
access-list OUTSIDE extended permit tcp object Branches-ALL object MSExchange object-group
DM_INLINE_TCP_2
access-list OUTSIDE remark Allow Applications
access-list OUTSIDE extended permit tcp object Branches-ALL object-group
DM_INLINE_NETWORK_9 eq https
access-list OUTSIDE remark Drop all other traffic
access-list OUTSIDE extended deny ip any any log
pager lines 24
logging enable
logging host inside 192.168.42.124
logging host inside 192.168.42.139
mtu outside 1500
mtu inside 1500
failover
failover lan unit primary
failover lan interface folink GigabitEthernet0/3
failover link folink GigabitEthernet0/3
failover interface ip folink 192.168.12.20 255.255.255.0 standby 192.168.12.21
icmp unreachable rate-limit 1 burst-size 1
icmp permit any outside
icmp permit any inside
asdm image disk0:/asdm-711.bin
asdm history enable
arp timeout 14400
no arp permit-nonconnected
access-group OUTSIDE in interface outside
access-group INSIDE in interface inside
route inside 0.0.0.0 0.0.0.0 192.168.11.60 1
route outside 10.10.0.0 255.255.0.0 192.168.11.1 1
route inside 10.10.0.0 255.255.255.0 192.168.11.60 1
route outside 10.10.1.0 255.255.255.0 192.168.11.2 1
route outside 10.10.2.0 255.255.255.0 192.168.11.3 1
route inside 10.10.3.0 255.255.255.0 192.168.11.60 1
route inside 10.10.4.0 255.255.255.0 192.168.11.60 1
route outside 10.10.254.0 255.255.255.0 192.168.11.3 1
route outside 10.10.255.0 255.255.255.0 192.168.11.2 1
route inside 192.168.0.0 255.255.0.0 192.168.11.10 1
route outside 192.168.1.111 255.255.255.255 192.168.11.2 1
route outside 192.168.1.112 255.255.255.255 192.168.11.3 1
route inside 192.168.20.0 255.255.252.0 192.168.11.60 1
```

```
route inside 192.168.24.0 255.255.255.0 192.168.11.60 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
aaa-server CiscoACS protocol tacacs+
aaa-server CiscoACS (inside) host 192.168.42.131
 key *****
user-identity default-domain LOCAL
aaa authentication ssh console CiscoACS LOCAL
aaa authentication enable console CiscoACS LOCAL
aaa authentication http console CiscoACS LOCAL
aaa accounting ssh console CiscoACS
aaa accounting enable console CiscoACS
aaa accounting command privilege 15 CiscoACS
aaa authentication secure-http-client
aaa local authentication attempts max-fail 6
aaa authorization exec authentication-server
http server enable
http server idle-timeout 15
http server session-timeout 60
http 192.168.41.102 255.255.255.255 inside
http 192.168.41.101 255.255.255.255 inside
http 192.168.42.122 255.255.255.255 inside
http 192.168.42.124 255.255.255.255 inside
http 192.168.42.133 255.255.255.255 inside
http 192.168.42.138 255.255.255.255 inside
http 192.168.42.139 255.255.255.255 inside
http 192.168.42.134 255.255.255.255 inside
snmp-server group V3Group v3 priv
snmp-server user csmadmin V3Group v3 encrypted auth sha
9e:72:6a:fa:06:f5:29:f9:8a:87:ce:fa:46:19:a5:80:6c:2d:2e:b8 priv aes 256
9e:72:6a:fa:06:f5:29:f9:8a:87:ce:fa:46:19:a5:80:6c:2d:2e:b8:bb:47:d1:68:d7:39:58:f4:62:f7:
38:36
snmp-server user ciscolms V3Group v3 encrypted auth sha
9e:72:6a:fa:06:f5:29:f9:8a:87:ce:fa:46:19:a5:80:6c:2d:2e:b8 priv aes 256
9e:72:6a:fa:06:f5:29:f9:8a:87:ce:fa:46:19:a5:80:6c:2d:2e:b8:bb:47:d1:68:d7:39:58:f4:62:f7:
38:36
snmp-server host inside 192.168.42.134 version 3 ciscolms
snmp-server host inside 192.168.42.139 version 3 ciscolms
snmp-server host inside 192.168.42.133 version 3 csmadmin
snmp-server location Building SJC-17-1 Aisle 1 Rack 3
snmp-server contact EmployeeA
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
snmp-server enable traps syslog
snmp-server enable traps ipsec start stop
snmp-server enable traps memory-threshold
snmp-server enable traps interface-threshold
snmp-server enable traps remote-access session-threshold-exceeded
snmp-server enable traps connection-limit-reached
snmp-server enable traps cpu threshold rising
snmp-server enable traps ikev2 start stop
snmp-server enable traps nat packet-discard
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 1
ssh scopy enable
ssh 192.168.41.101 255.255.255.255 inside
ssh 192.168.41.102 255.255.255.255 inside
```

```
ssh 192.168.42.122 255.255.255.255 inside
ssh 192.168.42.124 255.255.255.255 inside
ssh 192.168.42.133 255.255.255.255 inside
ssh 192.168.42.138 255.255.255.255 inside
ssh 192.168.42.139 255.255.255.255 inside
ssh 192.168.42.134 255.255.255.255 inside
ssh timeout 15
ssh version 2
console timeout 15
!
tls-proxy maximum-session 1000
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 192.168.62.162 source inside
ntp server 192.168.62.161 source inside prefer
ssl encryption aes256-sha1 3des-sha1
username csmadmin password <removed> privilege 15
username ciscolms password <removed> privilege 15
username bmcgloth password <removed> privilege 15
!
class-map inspection_default
 match default-inspection-traffic
class-map global-class-XXX
 match any
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 description IPS inspection policy for Cisco LAB
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
 class global-class-XXX
  ips promiscuous fail-open
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
```

```
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
password encryption aes
Cryptochecksum:74ca008c5477bc602c2080c680584775
: end
```

ASA-WAN-1_IDS

```
! ------------------------------
! Current configuration last modified Fri Dec 07 09:38:41 2012
! ------------------------------
! Version 7.1(6)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S648.0   2012-05-30
! ------------------------------
service interface
exit
! ------------------------------
service authentication
attemptLimit 6
password-strength
size 7-64
digits-min 1
lowercase-min 1
other-min 1
number-old-passwords 4
exit
cli-inactivity-timeout 15
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 192.168.11.23/24,192.168.11.10
host-name IPS-WAN-1
telnet-option disabled
access-list 192.168.41.101/32
access-list 192.168.41.102/32
access-list 192.168.42.122/32
access-list 192.168.42.124/32
access-list 192.168.42.133/32
access-list 192.168.42.134/32
access-list 192.168.42.138/32
access-list 192.168.42.139/32
login-banner-text WARNING: THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS
ONLY!
dns-primary-server enabled
address 192.168.42.130
exit
dns-secondary-server disabled
dns-tertiary-server disabled
exit
time-zone-settings
offset -480
standard-time-zone-name PST
exit
ntp-option enabled-ntp-unauthenticated
```

```
ntp-server 192.168.62.161
exit
summertime-option recurring
summertime-zone-name PDT
start-summertime
month march
week-of-month second
day-of-week sunday
time-of-day 02:00:00
exit
end-summertime
month november
week-of-month first
day-of-week sunday
time-of-day 02:00:00
exit
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
trap-destinations 192.168.42.124
trap-community-name RSAenvision
exit
enable-notifications true
trap-community-name RSAenvision
system-location Building SJC-17-1 Row 1 Rack 1
system-contact EmployeeA
exit
! ------------------------------
service signature-definition sig0
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
enable-tls true
port 443
server-id IPS-WAN-1
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
! ------------------------------
service global-correlation
exit
! ------------------------------
service aaa
aaa radius
```

```
primary-server
server-address 192.168.42.131
shared-secret <removed>
exit
nas-id IPS-WAN-1
local-fallback enabled
console-authentication radius-and-local
default-user-role administrator
exit
exit
! ----------------------------
service analysis-engine
exit
IPS-WAN-1#
```

RWAN-1

```
version 15.1
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
no platform punt-keepalive disable-kernel-core
!
hostname RWAN-1
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 50000
no logging rate-limit
enable secret 4 <removed>
!
aaa new-model
!
!
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
```

```
!
!
aaa session-id common
!
!
!
clock timezone PST -8 0
clock summer-time PSTDST recurring
ip source-route
!
!
!
no ip bootp server
no ip domain lookup
ip domain name cisco-irn.com
ip name-server 192.168.42.130
ip multicast-routing distributed
!
!
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
!
!
multilink bundle-name authenticated
!
password encryption aes
!
!
!
!
!
!
!
crypto pki trustpoint TP-self-signed-1264044905
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1264044905
 revocation-check none
 rsakeypair TP-self-signed-1264044905
!
!
crypto pki certificate chain TP-self-signed-1264044905
 certificate self-signed 01
  <removed>    quit
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
!
username bart privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 4 <removed>
username csmadmin privilege 15 secret 4 <removed>
!
redundancy
 mode none
!
!
!
ip ssh version 2
ip scp server enable
!
```

```
class-map match-all BRANCH-BULK-DATA
 match access-group name BULK-DATA-APPS
class-map match-all BULK-DATA
 match ip dscp af11  af12
class-map match-all INTERACTIVE-VIDEO
 match ip dscp af41  af42
class-map match-any BRANCH-TRANSACTIONAL-DATA
 match protocol telnet
 match access-group name TRANSACTIONAL-DATA-APPS
class-map match-all BRANCH-MISSION-CRITICAL
 match access-group name MISSION-CRITICAL-SERVERS
class-map match-all VOICE
 match ip dscp ef
class-map match-all MISSION-CRITICAL-DATA
 match ip dscp 25
class-map match-any BRANCH-NET-MGMT
 match protocol dns
 match access-group name NET-MGMT-APPS
class-map match-all ROUTING
 match ip dscp cs6
class-map match-all SCAVENGER
 match ip dscp cs1
class-map match-all NET-MGMT
 match ip dscp cs2
class-map match-any BRANCH-SCAVENGER
class-map match-any CALL-SIGNALING
 match ip dscp cs3
class-map match-all TRANSACTIONAL-DATA
 match ip dscp af21  af22
!
policy-map DataCenter-LAN-EDGE-OUT
 class class-default
policy-map DataCenter-LAN-EDGE-IN
 class BRANCH-MISSION-CRITICAL
  set ip dscp 25
 class BRANCH-TRANSACTIONAL-DATA
  set ip dscp af21
 class BRANCH-NET-MGMT
  set ip dscp cs2
 class BRANCH-BULK-DATA
  set ip dscp af11
 class BRANCH-SCAVENGER
  set ip dscp cs1
policy-map DataCenter-WAN-EDGE
 class VOICE
  priority percent 18
 class INTERACTIVE-VIDEO
  priority percent 15
 class CALL-SIGNALING
  bandwidth percent 5
 class ROUTING
  bandwidth percent 3
 class NET-MGMT
  bandwidth percent 2
 class MISSION-CRITICAL-DATA
  bandwidth percent 15
  random-detect
 class TRANSACTIONAL-DATA
  bandwidth percent 1
  random-detect dscp-based
 class class-default
  bandwidth percent 25
  random-detect
!
```

```
!
!
!
!
!
!
!
interface Loopback0
 ip address 192.168.1.111 255.255.255.255
!
interface GigabitEthernet0/0/0
 description SWAN-1
 ip address 192.168.11.2 255.255.255.0
 standby 1 ip 192.168.11.1
 standby 1 priority 105
 standby 1 preempt
 no negotiation auto
 service-policy input DataCenter-LAN-EDGE-IN
 service-policy output DataCenter-LAN-EDGE-OUT
!
interface GigabitEthernet0/0/1
 no ip address
 no negotiation auto
!
interface GigabitEthernet0/0/2
 description RSP-1 G0/1
 ip address 10.10.1.6 255.255.255.0
 no negotiation auto
 service-policy output DataCenter-WAN-EDGE
!
interface GigabitEthernet0/0/3
 no ip address
 shutdown
 no negotiation auto
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
!
no ip forward-protocol nd
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication CiscoACS
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip route 0.0.0.0 0.0.0.0 192.168.11.60
ip route 10.10.0.0 255.255.0.0 10.10.1.1
ip route 10.10.0.0 255.255.0.0 192.168.11.3 50
ip route 10.10.0.0 255.255.255.0 192.168.11.60
ip route 10.10.2.0 255.255.255.0 192.168.11.3
ip route 10.10.3.0 255.255.255.0 192.168.11.60
ip route 10.10.4.0 255.255.255.0 192.168.11.60
ip route 10.10.110.2 255.255.255.255 192.168.11.3
ip route 10.10.126.2 255.255.255.255 192.168.11.3
ip route 10.10.254.0 255.255.255.0 192.168.11.3
ip route 192.168.0.0 255.255.0.0 192.168.11.10
ip route 192.168.1.112 255.255.255.255 192.168.11.3
ip route 192.168.20.0 255.255.252.0 192.168.11.60
ip route 192.168.24.0 255.255.255.0 192.168.11.60
ip tacacs source-interface Loopback0
```

```
!
ip access-list extended BULK-DATA-APPS
 remark ---File Transfer---
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
 remark ---E-mail traffic---
 permit tcp any any eq smtp
 permit tcp any any eq pop3
 permit tcp any any eq 143
 remark ---other EDM app protocols---
 permit tcp any any range 3460 3466
 permit tcp any range 3460 3466 any
 remark ---messaging services---
 permit tcp any any eq 2980
 permit tcp any eq 2980 any
 remark ---Microsoft file services---
 permit tcp any any range 137 139
 permit tcp any range 137 139 any
ip access-list extended MISSION-CRITICAL-SERVERS
 remark ---POS Applications---
 permit ip 192.168.52.0 0.0.0.255 any
ip access-list extended NET-MGMT-APPS
 remark - Router user Authentication - Identifies TACACS Control traffic
 permit tcp any any eq tacacs
 permit tcp any eq tacacs any
ip access-list extended TRANSACTIONAL-DATA-APPS
 remark ---Workbrain Application---
 remark --Large Store Clock Server to Central Clock Application
 permit tcp host 192.168.46.72 eq 8444 host 10.10.49.94
 remark --Large branch Clock Server to CUAE
 permit tcp host 192.168.45.185 eq 8000 host 10.10.49.94
 remark ---LiteScape Application---
 permit ip host 192.168.46.82 any
 permit ip 239.192.0.0 0.0.0.255 any
 permit ip host 239.255.255.250 any
 remark ---Remote Desktop---
 permit tcp any any eq 3389
 permit tcp any eq 3389 any
 remark ---Oracle SIM---
 permit tcp 192.168.46.0 0.0.0.255 eq 7777 any
 permit tcp 192.168.46.0 0.0.0.255 eq 6003 any
 permit tcp 192.168.46.0 0.0.0.255 range 12401 12500 any
!
logging esm config
logging trap debugging
logging source-interface Loopback0
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
cdp run
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
```

```
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps ipsla
snmp-server enable traps syslog
snmp-server enable traps flash insertion removal
snmp-server host 192.168.42.124 remoteuser
!
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
!
!
control-plane
!
!
!
!
banner exec C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner incoming C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner login C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
```

```
!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication CiscoACS
 stopbits 1
line aux 0
 session-timeout 1  output
 exec-timeout 0 1
 privilege level 0
 no exec
 transport preferred none
 transport output none
 stopbits 1
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
!
ntp clock-period 17186047
ntp source Loopback0
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end
```

RWAN-2

```
version 15.1
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
no platform punt-keepalive disable-kernel-core
!
hostname RWAN-2
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-intf
 !
```

```
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 50000
no logging rate-limit
enable secret 5 <removed>
!
aaa new-model
!
!
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
aaa session-id common
!
!
clock timezone PST -8 0
clock summer-time PST recurring
ip source-route
!
!
no ip bootp server
no ip domain lookup
ip domain name cisco-irn.com
ip name-server 192.168.42.130
ip multicast-routing distributed
!
!
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
!
multilink bundle-name authenticated
!
password encryption aes
!
!
crypto pki trustpoint TP-self-signed-1414178861
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1414178861
 revocation-check none
 rsakeypair TP-self-signed-1414178861
!
!
crypto pki certificate chain TP-self-signed-1414178861
 certificate self-signed 01
  <removed>
    quit
archive
 log config
  logging enable
```

```
  notify syslog contenttype plaintext
  hidekeys
!
username bart privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 4 <removed>
username csmadmin privilege 15 secret 4 <removed>
!
redundancy
 mode none
!
!
!
ip ssh version 2
ip scp server enable
!
!
!
!
!
!
!
interface Loopback0
 ip address 192.168.1.112 255.255.255.255
 ip pim sparse-dense-mode
!
interface GigabitEthernet0/0/0
 description SWAN-2
 ip address 192.168.11.3 255.255.255.0
 standby 1 ip 192.168.11.1
 standby 1 priority 95
 no negotiation auto
!
interface GigabitEthernet0/0/1
 no ip address
 no negotiation auto
!
interface GigabitEthernet0/0/2
 description RSP-2 G0/1
 ip address 10.10.2.6 255.255.255.0
 no negotiation auto
!
interface GigabitEthernet0/0/3
 no ip address
 no negotiation auto
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
!
no ip forward-protocol nd
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication CiscoACS
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip route 0.0.0.0 0.0.0.0 192.168.11.60
ip route 10.10.0.0 255.255.0.0 10.10.2.1
ip route 10.10.0.0 255.255.0.0 192.168.11.2 50
ip route 10.10.0.0 255.255.255.0 192.168.11.60
ip route 10.10.1.0 255.255.255.0 192.168.11.2
```

```
ip route 10.10.3.0 255.255.255.0 192.168.11.60
ip route 10.10.4.0 255.255.255.0 192.168.11.60
ip route 10.10.110.1 255.255.255.255 192.168.11.2
ip route 10.10.126.1 255.255.255.255 192.168.11.2
ip route 10.10.255.0 255.255.255.0 192.168.11.2
ip route 192.168.0.0 255.255.0.0 192.168.11.10
ip route 192.168.1.111 255.255.255.255 192.168.11.2
ip route 192.168.20.0 255.255.252.0 192.168.11.60
ip route 192.168.24.0 255.255.255.0 192.168.11.60
ip tacacs source-interface Loopback0
!
!
logging esm config
logging trap debugging
logging source-interface Loopback0
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps ipsla
snmp-server enable traps syslog
snmp-server enable traps flash insertion removal
snmp-server host 192.168.42.124 remoteuser
!
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
!
!
control-plane
!
!
!
!
banner exec C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
```

```
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner incoming C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner login C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!


!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication CiscoACS
 stopbits 1
line aux 0
 session-timeout 1  output
 exec-timeout 0 1
 privilege level 0
 login authentication CiscoACS
 no exec
 transport preferred none
 transport output none
 stopbits 1
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
```

```
 transport preferred none
 transport input ssh
 transport output none
!
ntp clock-period 17219603
ntp source Loopback0
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end
```

SWAN-1

```
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
!
hostname SWAN-1
!
boot-start-marker
boot-end-marker
!
logging buffered 51200
enable secret 5 <removed>
!
username bart privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
username ciscolms privilege 15 secret 5 <removed>
!
!
aaa new-model
!
!
aaa group server tacacs+ PRIMARY1
!
aaa authentication login CiscoACS group PRIMARY1 local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PST recurring
switch 1 provision ws-c3750x-48p
switch 2 provision ws-c3750x-48p
system mtu routing 1500
authentication mac-move permit
ip subnet-zero
no ip source-route
no ip gratuitous-arps
```

```
!
!
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
password encryption aes
!
crypto pki trustpoint TP-self-signed-722491520
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-722491520
 revocation-check none
 rsakeypair TP-self-signed-722491520
!
!
crypto pki certificate chain TP-self-signed-722491520
 certificate self-signed 01
<removed>
  quit
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
spanning-tree mode pvst
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 10
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh version 2
ip scp server enable
!
!
interface GigabitEthernet1/0/1
 description Link to RWAN-1 G0-0-0
!
interface GigabitEthernet1/0/2
description Link to ASA-WAN-1 G0-0
!    |
!<removed for brevity>
!    |
interface GigabitEthernet1/0/48
shutdown
!
interface GigabitEthernet1/1/1
shutdown
!
interface GigabitEthernet1/1/2
shutdown
!
interface GigabitEthernet1/1/3
shutdown
!
interface GigabitEthernet1/1/4
```

```
shutdown
!
interface TenGigabitEthernet1/1/1
shutdown
!
interface TenGigabitEthernet1/1/2
shutdown
!
!
interface GigabitEthernet2/0/1
 description Link to RWAN-2 G0-0-0
!
interface GigabitEthernet2/0/2
description Link to ASA-WAN-2 G0-0
!
! <removed for brevity>
!
interface GigabitEthernet2/0/48
shutdown
!
interface GigabitEthernet2/1/1
shutdown
!
interface GigabitEthernet2/1/2
shutdown
!
interface GigabitEthernet2/1/3
shutdown
!
interface GigabitEthernet2/1/4
shutdown
!
interface TenGigabitEthernet2/1/1
shutdown
!
interface TenGigabitEthernet2/1/2
shutdown
!
!
interface Vlan1
 ip address 192.168.11.14 255.255.255.0
!
ip default-gateway 192.168.11.10
ip classless
no ip forward-protocol nd
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication CiscoACS
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
!
!
ip sla enable reaction-alerts
logging trap debugging
logging 192.168.42.124
logging 192.168.42.139
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
```

```
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 192.168.42.139 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 permit 192.168.42.139 log
access-list 88 deny   any log
snmp-server group V3Group v3 priv read V3Read write V3Write notify
*tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
snmp-server view V3Read iso included
snmp-server view V3Write iso included
snmp-server packetsize 8192
snmp-server location Building SJC-17-1 Aisle 2 Rack 3
snmp-server contact Bart McGlothin
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps power-ethernet group 1-4
snmp-server enable traps power-ethernet police
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps hsrp
snmp-server enable traps energywise
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps rtr
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 192.168.42.134 version 3 priv ciscolms
snmp-server host 192.168.42.139 version 3 priv ciscolms
snmp-server host 192.168.42.133 version 3 priv csmadmin
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
!
banner exec ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
```

```
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication CiscoACS
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
!
!
monitor session 1 source interface Fa1/0/1
monitor session 1 destination interface Fa1/0/48
ntp clock-period 36029318
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end
```

SWAN-3

```
Current configuration : 12174 bytes
!
! Last configuration change at 14:08:38 PST Fri Dec 21 2012 by bmcgloth
! NVRAM config last updated at 13:54:15 PST Fri Dec 21 2012 by bmcgloth
!
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
!
hostname SWAN-3
!
boot-start-marker
```

```
boot-end-marker
!
logging buffered 51200
enable secret 5 <removed>
!

username bart privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
username ciscolms privilege 15 secret 5 <removed>
!
!
aaa new-model
!
!
aaa group server tacacs+ PRIMARY1
!
aaa authentication login CiscoACS group PRIMARY1 local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PST recurring
switch 1 provision ws-c3750x-48p
switch 2 provision ws-c3750x-48p
system mtu routing 1500
authentication mac-move permit
ip subnet-zero
no ip source-route
no ip gratuitous-arps
!
!
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
password encryption aes
!
crypto pki trustpoint TP-self-signed-722491520
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-722491520
 revocation-check none
 rsakeypair TP-self-signed-722491520
!
!
crypto pki certificate chain TP-self-signed-722491520
 certificate self-signed 01
<removed>
  quit
!
!
!
archive
 log config
```

```
  logging enable
  notify syslog contenttype plaintext
  hidekeys
spanning-tree mode pvst
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 10
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh version 2
ip scp server enable
!
!
interface GigabitEthernet1/0/1
 description Link to RCORE-2 G1-1
!
interface GigabitEthernet1/0/2
description Link to ASA-WAN-1 G0-1
!    |
!<removed for brevity>
!    |
interface GigabitEthernet1/0/48
shutdown
!
interface GigabitEthernet1/1/1
shutdown
!
interface GigabitEthernet1/1/2
shutdown
!
interface GigabitEthernet1/1/3
shutdown
!
interface GigabitEthernet1/1/4
shutdown
!
interface TenGigabitEthernet1/1/1
shutdown
!
interface TenGigabitEthernet1/1/2
shutdown
!
!
interface GigabitEthernet2/0/1
 description Link to RCORE-1 G1-1
!
interface GigabitEthernet2/0/2
description Link to ASA-WAN-2 G0-1
!
! <removed for brevity>
!
interface GigabitEthernet2/0/48
shutdown
!
interface GigabitEthernet2/1/1
shutdown
!
interface GigabitEthernet2/1/2
shutdown
!
interface GigabitEthernet2/1/3
```

```
shutdown
!
interface GigabitEthernet2/1/4
shutdown
!
interface TenGigabitEthernet2/1/1
shutdown
!
interface TenGigabitEthernet2/1/2
shutdown
!
!
interface Vlan1
 ip address 192.168.11.14 255.255.255.0
!
ip default-gateway 192.168.11.10
ip classless
no ip forward-protocol nd
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication CiscoACS
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
!
!
ip sla enable reaction-alerts
logging trap debugging
logging 192.168.42.124
logging 192.168.42.139
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 192.168.42.139 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 permit 192.168.42.139 log
access-list 88 deny   any log
snmp-server group V3Group v3 priv read V3Read write V3Write notify
*tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
snmp-server view V3Read iso included
snmp-server view V3Write iso included
snmp-server packetsize 8192
snmp-server location Building SJC-17-1 Aisle 2 Rack 3
snmp-server contact Bart McGlothin
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps power-ethernet group 1-4
snmp-server enable traps power-ethernet police
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps config-copy
```

```
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps hsrp
snmp-server enable traps energywise
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps rtr
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 192.168.42.134 version 3 priv ciscolms
snmp-server host 192.168.42.139 version 3 priv ciscolms
snmp-server host 192.168.42.133 version 3 priv csmadmin
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
!
banner exec ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication CiscoACS
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
```

```
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
!
!
monitor session 1 source interface Fa1/0/1
monitor session 1 destination interface Fa1/0/48
ntp clock-period 36029318
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end
```

Core

RCORE-1

```
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
service counters max age 5
!
hostname RCORE-1
!
boot-start-marker
boot system flash disk0:s72033-adventerprisek9_wan-mz.122-33.SXJ.bin
boot-end-marker
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 50000
no logging rate-limit
enable secret 5 <removed>
!
username bart privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
aaa new-model
!
!
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
```

```
clock timezone PST -8
clock summer-time PSTDST recurring
ip wccp 61
ip wccp 62
!
!
!
no ip bootp server
ip multicast-routing
ip ssh version 2
ip scp server enable
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
ipv6 mfib hardware-switching replication-mode ingress
vtp domain COMPLIANCEVTP
vtp mode transparent
mls ip cef load-sharing full simple
no mls acl tcam share-global
mls netflow interface
mls cef error action freeze
password encryption aes
!
crypto pki trustpoint TP-self-signed-1104
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1104
 revocation-check none
 rsakeypair TP-self-signed-1104
!
!
crypto pki certificate chain TP-self-signed-1104
 certificate self-signed 01
  <removed>
  quit
!
!
!
!
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
!
spanning-tree mode rapid-pvst
spanning-tree loopguard default
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
spanning-tree pathcost method long
environment temperature-controlled
diagnostic bootup level minimal
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
```

```
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
redundancy
 main-cpu
  auto-sync running-config
 mode sso
!
!
vlan internal allocation policy descending
vlan dot1q tag native
vlan access-log ratelimit 2000
!
!
!
!
!
interface Loopback0
 ip address 192.168.1.1 255.255.255.255
!
interface Port-channel99
 ip address 192.168.10.29 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-dense-mode
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 7 <removed>
 ip ospf network point-to-point
 ip ospf hello-interval 2
 ip ospf dead-interval 6
 logging event link-status
!
interface GigabitEthernet1/1
 description to DC WAN_SWAN-3
 ip address 192.168.11.11 255.255.255.0
 standby 0 ip 192.168.11.10
 standby 0 priority 101
 standby 0 preempt
!
interface GigabitEthernet1/2
 no ip address
 shutdown
!
interface GigabitEthernet1/3
 no ip address
 shutdown
!
interface GigabitEthernet1/4
 no ip address
 shutdown
!
interface GigabitEthernet1/5
 no ip address
 shutdown
!
interface GigabitEthernet1/6
 no ip address
 shutdown
!
interface GigabitEthernet1/7
```

```
 no ip address
 shutdown
!
interface GigabitEthernet1/8
 no ip address
 shutdown
!
interface GigabitEthernet1/9
 no ip address
 shutdown
!
interface GigabitEthernet1/10
 no ip address
 shutdown
!
interface GigabitEthernet1/11
 no ip address
 shutdown
!
interface GigabitEthernet1/12
 no ip address
 shutdown
!
interface GigabitEthernet1/13
 no ip address
 shutdown
!
interface GigabitEthernet1/14
 no ip address
 shutdown
!
interface GigabitEthernet1/15
 no ip address
 shutdown
!
interface GigabitEthernet1/16
 no ip address
 shutdown
!
interface GigabitEthernet1/17
 no ip address
 shutdown
!
interface GigabitEthernet1/18
 no ip address
 shutdown
!
interface GigabitEthernet1/19
 no ip address
 shutdown
!
interface GigabitEthernet1/20
 no ip address
 shutdown
!
interface GigabitEthernet1/21
 no ip address
 shutdown
!
interface GigabitEthernet1/22
 no ip address
 shutdown
!
interface GigabitEthernet1/23
```

```
 no ip address
 shutdown
!
interface GigabitEthernet1/24
 no ip address
 shutdown
!
interface GigabitEthernet1/25
 no ip address
 shutdown
!
interface GigabitEthernet1/26
 no ip address
 shutdown
!
interface GigabitEthernet1/27
 no ip address
 shutdown
!
interface GigabitEthernet1/28
 no ip address
 shutdown
!
interface GigabitEthernet1/29
 no ip address
 shutdown
!
interface GigabitEthernet1/30
 no ip address
 shutdown
!
interface GigabitEthernet1/31
 no ip address
 shutdown
!
interface GigabitEthernet1/32
 no ip address
 shutdown
!
interface GigabitEthernet1/33
 no ip address
 shutdown
!
interface GigabitEthernet1/34
 no ip address
 shutdown
!
interface GigabitEthernet1/35
 no ip address
 shutdown
!
interface GigabitEthernet1/36
 no ip address
 shutdown
!
interface GigabitEthernet1/37
 no ip address
 shutdown
!
interface GigabitEthernet1/38
 no ip address
 shutdown
!
interface GigabitEthernet1/39
```

```
 no ip address
 shutdown
!
interface GigabitEthernet1/40
 no ip address
 shutdown
!
interface GigabitEthernet1/41
 no ip address
 shutdown
!
interface GigabitEthernet1/42
 no ip address
 shutdown
!
interface GigabitEthernet1/43
 no ip address
 shutdown
!
interface GigabitEthernet1/44
 no ip address
 shutdown
!
interface GigabitEthernet1/45
 no ip address
 shutdown
!
interface GigabitEthernet1/46
 no ip address
 shutdown
!
interface GigabitEthernet1/47
 no ip address
 shutdown
!
interface GigabitEthernet1/48
 no ip address
 shutdown
!
interface TenGigabitEthernet2/1
 description 10Gig LINK to RAGG-1 T1/3
 ip address 192.168.10.13 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-dense-mode
 ip igmp query-interval 125
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 7 <removed>
 ip ospf network point-to-point
 ip ospf hello-interval 2
 ip ospf dead-interval 6
 logging event link-status
!
interface TenGigabitEthernet2/2
 description 10Gig LINK to RAGG-2 T1/3
 ip address 192.168.10.17 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-dense-mode
 ip igmp query-interval 125
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 7 <removed>
 ip ospf network point-to-point
 ip ospf hello-interval 2
```

```
 ip ospf dead-interval 6
 logging event link-status
!
interface TenGigabitEthernet2/3
 description 10Gig LINK to RCORE-2
 no ip address
 channel-group 99 mode active
!
interface TenGigabitEthernet2/4
 description 10Gig LINK to RCORE-2
 no ip address
 channel-group 99 mode active
!
interface TenGigabitEthernet2/5
 no ip address
 shutdown
!
interface TenGigabitEthernet2/6
 no ip address
 shutdown
!
interface TenGigabitEthernet2/7
 no ip address
 shutdown
!
interface TenGigabitEthernet2/8
 no ip address
 shutdown
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 no ip address
 shutdown
!
interface GigabitEthernet6/1
 no ip address
 shutdown
!
interface GigabitEthernet6/2
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 5
 router-id 192.168.1.1
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 nsf
 redistribute static subnets
 passive-interface default
 no passive-interface TenGigabitEthernet2/1
 no passive-interface TenGigabitEthernet2/2
 no passive-interface Port-channel99
 network 192.168.0.0 0.0.255.255 area 0
 default-information originate metric 20 metric-type 1
!
ip classless
no ip forward-protocol nd
```

```
ip route 0.0.0.0 0.0.0.0 192.168.11.60 name default-to-internet
ip route 10.10.0.0 255.255.0.0 192.168.11.1 name route-to-branchs
ip route 10.10.0.0 255.255.255.0 192.168.11.60 name route-to-SP
ip route 10.10.1.0 255.255.255.0 192.168.11.2
ip route 10.10.2.0 255.255.255.0 192.168.11.3
ip route 10.10.110.1 255.255.255.255 192.168.11.2
ip route 10.10.110.2 255.255.255.255 192.168.11.3
ip route 10.10.126.1 255.255.255.255 192.168.11.2
ip route 10.10.126.2 255.255.255.255 192.168.11.3
ip route 10.10.254.0 255.255.255.0 192.168.11.3
ip route 10.10.255.0 255.255.255.0 192.168.11.2
ip route 192.168.1.111 255.255.255.255 192.168.11.2
ip route 192.168.1.112 255.255.255.255 192.168.11.3
ip route 192.168.20.0 255.255.255.0 192.168.11.60 name route-to-DMZ
ip route 192.168.21.0 255.255.255.0 192.168.11.60 name route-to-DMZ
ip route 192.168.22.0 255.255.255.0 192.168.11.60 name route-to-DMZ
ip route 192.168.23.0 255.255.255.0 192.168.11.60 name route-to-DMZ
!
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication CiscoACS
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip pim send-rp-discovery scope 2
ip tacacs source-interface Loopback0
!
logging trap debugging
logging source-interface Loopback0
logging 192.168.42.124
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps hsrp
snmp-server enable traps MAC-Notification change move threshold
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps energywise
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps port-security
snmp-server enable traps errdisable
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
```

```
tacacs-server key 7 <removed>
!
!
control-plane
!
!
dial-peer cor custom
!
!
!
banner exec C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner incoming C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner login C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!


!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication CiscoACS
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
```

```
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
!
!
ntp source Loopback0
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162
mac-address-table aging-time 480
!
end
```

RCORE-2

```
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
service counters max age 5
!
hostname RCORE-2
!
boot-start-marker
boot system flash disk1:s72033-adventerprisek9_wan-mz.122-33.SXJ.bin
boot-end-marker
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 50000
no logging rate-limit
enable secret 5 <removed>
!
username bart privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
aaa new-model
!
!
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
call-home
 no alert-group configuration
```

```
 no alert-group diagnostic
 no alert-group environment
 no alert-group inventory
 no alert-group syslog
ip wccp 61
ip wccp 62
!
!
!
no ip bootp server
ip multicast-routing
ip ssh version 2
ip scp server enable
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
ipv6 mfib hardware-switching replication-mode ingress
vtp domain COMPLIANCEVTP
vtp mode transparent
mls ip cef load-sharing full simple
no mls acl tcam share-global
mls netflow interface
mls cef error action freeze
password encryption aes
!
crypto pki trustpoint TP-self-signed-1051
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1051
 revocation-check none
 rsakeypair TP-self-signed-1051
!
!
crypto pki certificate chain TP-self-signed-1051
 certificate self-signed 01
  <removed>
  quit
!
!
!
!
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
!
spanning-tree mode rapid-pvst
spanning-tree loopguard default
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
spanning-tree pathcost method long
environment temperature-controlled
diagnostic bootup level minimal
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
```

```
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
redundancy
 main-cpu
  auto-sync running-config
 mode sso
!
!
vlan internal allocation policy descending
vlan dot1q tag native
vlan access-log ratelimit 2000
!
!
!
!
!
interface Loopback0
 ip address 192.168.1.2 255.255.255.255
!
interface Port-channel99
 description link between CORE's
 ip address 192.168.10.30 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-dense-mode
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 7 <removed>
 ip ospf network point-to-point
 ip ospf hello-interval 2
 ip ospf dead-interval 6
 logging event link-status
!
interface GigabitEthernet1/1
 description to DC WAN_SWAN-3/4
 ip address 192.168.11.12 255.255.255.0
 standby 0 ip 192.168.11.10
 standby 0 priority 99
 standby 0 preempt
!
interface GigabitEthernet1/2
 no ip address
 shutdown
!
interface GigabitEthernet1/3
 no ip address
 shutdown
!
interface GigabitEthernet1/4
 no ip address
 shutdown
!
interface GigabitEthernet1/5
 no ip address
 shutdown
!
interface GigabitEthernet1/6
 no ip address
```

```
 shutdown
!
interface GigabitEthernet1/7
 no ip address
 shutdown
!
interface GigabitEthernet1/8
 no ip address
 shutdown
!
interface GigabitEthernet1/9
 no ip address
 shutdown
!
interface GigabitEthernet1/10
 no ip address
 shutdown
!
interface GigabitEthernet1/11
 no ip address
 shutdown
!
interface GigabitEthernet1/12
 no ip address
 shutdown
!
interface GigabitEthernet1/13
 no ip address
 shutdown
!
interface GigabitEthernet1/14
 no ip address
 shutdown
!
interface GigabitEthernet1/15
 no ip address
 shutdown
!
interface GigabitEthernet1/16
 no ip address
 shutdown
!
interface GigabitEthernet1/17
 no ip address
 shutdown
!
interface GigabitEthernet1/18
 no ip address
 shutdown
!
interface GigabitEthernet1/19
 no ip address
 shutdown
!
interface GigabitEthernet1/20
 no ip address
 shutdown
!
interface GigabitEthernet1/21
 no ip address
 shutdown
!
interface GigabitEthernet1/22
 no ip address
```

```
 shutdown
!
interface GigabitEthernet1/23
 no ip address
 shutdown
!
interface GigabitEthernet1/24
 no ip address
 shutdown
!
interface GigabitEthernet1/25
 no ip address
 shutdown
!
interface GigabitEthernet1/26
 no ip address
 shutdown
!
interface GigabitEthernet1/27
 no ip address
 shutdown
!
interface GigabitEthernet1/28
 no ip address
 shutdown
!
interface GigabitEthernet1/29
 no ip address
 shutdown
!
interface GigabitEthernet1/30
 no ip address
 shutdown
!
interface GigabitEthernet1/31
 no ip address
 shutdown
!
interface GigabitEthernet1/32
 no ip address
 shutdown
!
interface GigabitEthernet1/33
 no ip address
 shutdown
!
interface GigabitEthernet1/34
 no ip address
 shutdown
!
interface GigabitEthernet1/35
 no ip address
 shutdown
!
interface GigabitEthernet1/36
 no ip address
 shutdown
!
interface GigabitEthernet1/37
 no ip address
 shutdown
!
interface GigabitEthernet1/38
 no ip address
```

```
 shutdown
!
interface GigabitEthernet1/39
 no ip address
 shutdown
!
interface GigabitEthernet1/40
 no ip address
 shutdown
!
interface GigabitEthernet1/41
 no ip address
 shutdown
!
interface GigabitEthernet1/42
 no ip address
 shutdown
!
interface GigabitEthernet1/43
 no ip address
 shutdown
!
interface GigabitEthernet1/44
 no ip address
 shutdown
!
interface GigabitEthernet1/45
 no ip address
 shutdown
!
interface GigabitEthernet1/46
 no ip address
 shutdown
!
interface GigabitEthernet1/47
 no ip address
 shutdown
!
interface GigabitEthernet1/48
 no ip address
 shutdown
!
interface TenGigabitEthernet2/1
 description 10Gig LINK to RAGG-1 T1/4
 ip address 192.168.10.21 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-dense-mode
 ip igmp query-interval 125
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 7 <removed>
 ip ospf network point-to-point
 ip ospf hello-interval 2
 ip ospf dead-interval 6
 logging event link-status
!
interface TenGigabitEthernet2/2
 description 10Gig LINK to RAGG-2 T1/4
 ip address 192.168.10.25 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip pim sparse-dense-mode
 ip igmp query-interval 125
 ip ospf authentication message-digest
```

```
 ip ospf message-digest-key 1 md5 7 <removed>
 ip ospf network point-to-point
 ip ospf hello-interval 2
 ip ospf dead-interval 6
 logging event link-status
!
interface TenGigabitEthernet2/3
 description 10Gig LINK to RCORE-1
 no ip address
 channel-group 99 mode active
!
interface TenGigabitEthernet2/4
 description 10Gig LINK to RCORE-1
 no ip address
 channel-group 99 mode active
!
interface TenGigabitEthernet2/5
 no ip address
 shutdown
!
interface TenGigabitEthernet2/6
 no ip address
 shutdown
!
interface TenGigabitEthernet2/7
 no ip address
 shutdown
!
interface TenGigabitEthernet2/8
 no ip address
 shutdown
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 no ip address
 shutdown
!
interface GigabitEthernet6/1
 no ip address
 shutdown
!
interface GigabitEthernet6/2
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 5
 router-id 192.168.1.2
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 nsf
 redistribute static subnets
 passive-interface default
 no passive-interface TenGigabitEthernet2/1
 no passive-interface TenGigabitEthernet2/2
 no passive-interface Port-channel99
 network 192.168.0.0 0.0.255.255 area 0
 default-information originate metric 22 metric-type 1
```

```
!
ip classless
no ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.11.60 name default-to-internet
ip route 10.10.0.0 255.255.0.0 192.168.11.1 name route-to-branchs
ip route 10.10.0.0 255.255.255.0 192.168.11.60 name route-to-SP
ip route 10.10.1.0 255.255.255.0 192.168.11.2
ip route 10.10.2.0 255.255.255.0 192.168.11.3
ip route 10.10.110.1 255.255.255.255 192.168.11.2
ip route 10.10.110.2 255.255.255.255 192.168.11.3
ip route 10.10.126.1 255.255.255.255 192.168.11.2
ip route 10.10.126.2 255.255.255.255 192.168.11.3
ip route 10.10.254.0 255.255.255.0 192.168.11.3
ip route 10.10.255.0 255.255.255.0 192.168.11.2
ip route 192.168.20.0 255.255.255.0 192.168.11.60 name route-to-DMZ
ip route 192.168.21.0 255.255.255.0 192.168.11.60 name route-to-DMZ
ip route 192.168.22.0 255.255.255.0 192.168.11.60 name route-to-DMZ
ip route 192.168.23.0 255.255.255.0 192.168.11.60 name route-to-DMZ
!
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication CiscoACS
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip pim send-rp-discovery scope 2
ip tacacs source-interface Loopback0
!
logging trap debugging
logging source-interface Loopback0
logging 192.168.42.124
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps hsrp
snmp-server enable traps MAC-Notification change move threshold
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps energywise
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps port-security
snmp-server enable traps errdisable
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131 timeout 5
```

```
tacacs-server directed-request
tacacs-server key 7 <removed>
!
!
control-plane
!
!
dial-peer cor custom
!
!
!
banner exec C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner incoming C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner login C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!


!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication CiscoACS
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
```

```
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
!
ntp source Loopback0
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162
mac-address-table aging-time 480
!
end
```

Aggregation

ASA-DC-1

```
: Saved
:
ASA Version 8.4(1) <context>
!
firewall transparent
hostname dca-vc1
domain-name cisco-irn.com
enable password <removed> encrypted
passwd <removed> encrypted
names
!
interface outside
 nameif north
 bridge-group 1
 security-level 0
!
interface inside
 nameif south
 bridge-group 1
 security-level 100
!
interface BVI1
 ip address 192.168.162.21 255.255.255.0 standby 192.168.162.22
!
dns domain-lookup south
dns server-group DefaultDNS
 name-server 192.168.42.130
 domain-name cisco-irn.com
object-group network AdminStation
 network-object 192.168.41.101 255.255.255.255
object-group network AdminStation2
 network-object 192.168.41.102 255.255.255.255
object-group network AdminStation4-bart
 network-object 10.19.151.99 255.255.255.255
object-group network CSM_INLINE_src_rule_77309411633
 description Generated by CS-Manager from src of FirewallRule# 2
(ASA-DC-1-vdc1_v1/mandatory)
 group-object AdminStation
 group-object AdminStation2
 group-object AdminStation4-bart
```

```
object-group network DC-ALL
 description All of the Data Center
 network-object 192.168.0.0 255.255.0.0
object-group network Branches-ALL
 description all branch networks
 network-object 10.10.0.0 255.255.0.0
object-group network CSM_INLINE_dst_rule_77309411633
 description Generated by CS-Manager from dst of FirewallRule# 2
(ASA-DC-1-vdc1_v1/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
object-group network EMC-NCM
 description EMC Network Configuration Manager
 network-object 192.168.42.122 255.255.255.255
object-group network CSManager
 description Cisco Security Manager
 network-object 192.168.42.133 255.255.255.255
object-group network RSA-enVision
 description RSA EnVision Syslog collector and SIM
 network-object 192.168.42.124 255.255.255.255
object-group network AdminStation3
 network-object 192.168.42.138 255.255.255.255
object-group network Admin-Systems
 group-object EMC-NCM
 group-object AdminStation
 group-object AdminStation2
 group-object CSManager
 group-object RSA-enVision
 group-object AdminStation3
 group-object AdminStation4-bart
object-group network DC-DMZ
 description (Optimized by CS-Manager)
 network-object 192.168.20.0 255.255.252.0
 network-object 192.168.24.0 255.255.255.0
object-group network CSM_INLINE_dst_rule_77309411635
 description Generated by CS-Manager from dst of FirewallRule# 3
(ASA-DC-1-vdc1_v1/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
 group-object DC-DMZ
object-group network CSM_INLINE_src_rule_77309414079
 description Generated by CS-Manager from src of FirewallRule# 4
(ASA-DC-1-vdc1_v1/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
object-group network CSM_INLINE_src_rule_77309414081
 description Generated by CS-Manager from src of FirewallRule# 5
(ASA-DC-1-vdc1_v1/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
object-group network ActiveDirectory.cisco-irn.com
 network-object 192.168.42.130 255.255.255.255
object-group network vSphere-1
 description vSphere server for Lab
 network-object 192.168.41.102 255.255.255.255
object-group network WCSManager
 description Wireless Manager
 network-object 192.168.43.135 255.255.255.255
object-group network DC-Wifi-Controllers
 description Central Wireless Controllers for branchs
 network-object 192.168.43.21 255.255.255.255
 network-object 192.168.43.22 255.255.255.255
object-group network DC-Wifi-MSE
 description Mobility Service Engines
```

```
 network-object 192.168.43.31 255.255.255.255
 network-object 192.168.43.32 255.255.255.255
object-group network CSM_INLINE_src_rule_77309411641
 description Generated by CS-Manager from src of FirewallRule# 9
(ASA-DC-1-vdc1_v1/mandatory)
 group-object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
object-group network PAME-DC-1
 network-object 192.168.44.111 255.255.255.255
object-group network MSP-DC-1
 description Data Center VSOM
 network-object 192.168.44.121 255.255.255.255
object-group network CSM_INLINE_src_rule_77309411643
 description Generated by CS-Manager from src of FirewallRule# 10
(ASA-DC-1-vdc1_v1/mandatory)
 group-object PAME-DC-1
 group-object MSP-DC-1
object-group network DC-WAAS
 description WAE Appliances in Data Center
 network-object 192.168.48.10 255.255.255.255
 network-object 192.168.49.10 255.255.255.255
 network-object 192.168.47.11 255.255.255.255
 network-object 192.168.47.12 255.255.255.255
object-group network CSM_INLINE_src_rule_77309414071
 description Generated by CS-Manager from src of FirewallRule# 15
(ASA-DC-1-vdc1_v1/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
object-group network NTP-Servers
 description NTP Servers
 network-object 192.168.62.161 255.255.255.255
 network-object 162.168.62.162 255.255.255.255
object-group network TACACS
 description Csico Secure ACS server for TACACS and Radius
 network-object 192.168.42.131 255.255.255.255
object-group network RSA-AM
 description RSA Authentication Manager for SecureID
 network-object 192.168.42.137 255.255.255.255
object-group network NAC-2
 network-object 192.168.42.112 255.255.255.255
object-group network NAC-1
 description ISE server for NAC
 network-object 192.168.42.111 255.255.255.255
object-group network CSM_INLINE_dst_rule_77309411663
 description Generated by CS-Manager from dst of FirewallRule# 25
(ASA-DC-1-vdc1_v1/mandatory)
 group-object TACACS
 group-object RSA-AM
 group-object NAC-2
 group-object NAC-1
object-group network CSM_INLINE_dst_rule_77309411665
 description Generated by CS-Manager from dst of FirewallRule# 26
(ASA-DC-1-vdc1_v1/mandatory)
 group-object NAC-2
 group-object NAC-1
object-group network CSM_INLINE_dst_rule_77309411669
 description Generated by CS-Manager from dst of FirewallRule# 28
(ASA-DC-1-vdc1_v1/mandatory)
 group-object PAME-DC-1
 group-object MSP-DC-1
object-group network CSM_INLINE_dst_rule_77309411671
 description Generated by CS-Manager from dst of FirewallRule# 29
(ASA-DC-1-vdc1_v1/mandatory)
```

```
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
object-group network MS-Update
 description Windows Update Server
 network-object 192.168.42.150 255.255.255.255
object-group network MSExchange
 description Mail Server
 network-object 192.168.42.140 255.255.255.255
object-group network POS-Store-Conv
 network-object 10.10.160.81 255.255.255.255
object-group network POS-Store-MSP
 network-object 10.10.176.81 255.255.255.255
object-group network POS-Store-SMALL-1
 description Small Store POS devices
 network-object 10.10.128.81 255.255.255.255
 network-object 10.10.128.82 255.255.255.255
object-group network POS-Store-Medium
 network-object 10.10.112.81 255.255.255.255
 network-object 10.10.125.40 255.255.255.255
object-group network POS-Store-Mini
 network-object 10.10.144.81 255.255.255.255
object-group network POS-Store-3g
 network-object 10.10.192.82 255.255.255.255
object-group network POS-Store-Large
 network-object 10.10.96.81 255.255.255.255
 network-object 10.10.96.82 255.255.255.255
object-group network CSM_INLINE_src_rule_77309411683
 description Generated by CS-Manager from src of FirewallRule# 35
(ASA-DC-1-vdc1_v1/mandatory)
 group-object POS-Store-Conv
 group-object POS-Store-MSP
 group-object POS-Store-SMALL-1
 group-object POS-Store-Medium
 group-object POS-Store-Mini
 group-object POS-Store-3g
 group-object POS-Store-Large
object-group network DC-POS-Tomax
 description Tomax POS Communication from Store to Data Center
 network-object 192.168.52.96 255.255.255.224
object-group network DC-POS
 description POS in the Data Center
 network-object 192.168.52.0 255.255.255.0
object-group network DC-POS-SAP
 description SAP POS Communication from Store to Data Center
 network-object 192.168.52.144 255.255.255.240
object-group network DC-POS-Oracle
 description Oracle POS Communication from Store to Data Center
 network-object 192.168.52.128 255.255.255.240
object-group network CSM_INLINE_dst_rule_77309411683
 description Generated by CS-Manager from dst of FirewallRule# 35
(ASA-DC-1-vdc1_v1/mandatory)
 group-object DC-POS-Tomax
 group-object DC-POS
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
object-group network CSM_INLINE_src_rule_77309414158
 description Generated by CS-Manager from src of FirewallRule# 36
(ASA-DC-1-vdc1_v1/mandatory)
 network-object 192.168.22.11 255.255.255.255
 network-object 192.168.22.12 255.255.255.255
 network-object 192.168.21.0 255.255.255.0
object-group network CSM_INLINE_src_rule_77309414160
 description Generated by CS-Manager from src of FirewallRule# 37
(ASA-DC-1-vdc1_v1/mandatory)
```

```
 network-object 192.168.22.11 255.255.255.255
 network-object 192.168.22.12 255.255.255.255
 network-object 192.168.21.0 255.255.255.0
object-group network CSM_INLINE_src_rule_77309414162
 description Generated by CS-Manager from src of FirewallRule# 38
(ASA-DC-1-vdc1_v1/mandatory)
 network-object 192.168.22.11 255.255.255.255
 network-object 192.168.22.12 255.255.255.255
 network-object 192.168.21.0 255.255.255.0
object-group service HTTPS-8443
 service-object tcp destination eq 8443
object-group service CSM_INLINE_svc_rule_77309411635
 description Generated by CS-Manager from service of FirewallRule# 3
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp destination eq ssh
 service-object tcp destination eq https
 group-object HTTPS-8443
object-group service CSM_INLINE_svc_rule_77309414079
 description Generated by CS-Manager from service of FirewallRule# 4
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp destination eq smtp
 service-object tcp destination eq https
 service-object tcp destination eq ssh
object-group service CSM_INLINE_svc_rule_77309414081
 description Generated by CS-Manager from service of FirewallRule# 5
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp destination eq https
 service-object tcp destination eq ssh
object-group service RPC
 service-object tcp destination eq 135
object-group service LDAP-GC
 service-object tcp destination eq 3268
object-group service LDAP-GC-SSL
 service-object tcp destination eq 3269
object-group service DNS-Resolving
 description Domain Name Server
 service-object tcp destination eq domain
 service-object udp destination eq domain
object-group service Kerberos-TCP
 service-object tcp destination eq 88
object-group service Microsoft-DS-SMB
 description Microsoft-DS Active Directory, Windows shares Microsoft-DS SMB file sharing
 service-object tcp destination eq 445
object-group service LDAP-UDP
 service-object udp destination eq 389
object-group service RPC-HighPorts
 service-object tcp destination range 1024 65535
object-group service CSM_INLINE_svc_rule_77309411637
 description Generated by CS-Manager from service of FirewallRule# 7
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp destination eq ldap
 service-object tcp destination eq ldaps
 service-object udp destination eq 88
 service-object udp destination eq ntp
 service-object udp destination eq netbios-dgm
 group-object RPC
 group-object LDAP-GC
 group-object LDAP-GC-SSL
 group-object DNS-Resolving
 group-object Kerberos-TCP
 group-object Microsoft-DS-SMB
 group-object LDAP-UDP
 group-object RPC-HighPorts
object-group service vCenter-to-ESX4
```

```
 description Communication from vCetner to ESX hosts
 service-object tcp destination eq 5989
 service-object tcp destination eq 8000
 service-object tcp destination eq 902
 service-object tcp destination eq 903
object-group service CSM_INLINE_svc_rule_77309411639
 description Generated by CS-Manager from service of FirewallRule# 8
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp destination eq https
 service-object tcp destination eq ssh
 group-object vCenter-to-ESX4
object-group service IP-Protocol-97
 description IP protocol 97
 service-object 97
object-group service TFTP
 description Trivial File Transfer
 service-object tcp destination eq 69
 service-object udp destination eq tftp
object-group service LWAPP
 description LWAPP UDP ports 12222 and 12223
 service-object udp destination eq 12222
 service-object udp destination eq 12223
object-group service CAPWAP
 description CAPWAP UDP ports 5246 and 5247
 service-object udp destination eq 5246
 service-object udp destination eq 5247
object-group service CSM_INLINE_svc_rule_77309411641
 description Generated by CS-Manager from service of FirewallRule# 9
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp destination eq https
 service-object tcp destination eq www
 service-object udp destination eq isakmp
 service-object tcp destination eq telnet
 service-object tcp destination eq ssh
 group-object IP-Protocol-97
 group-object TFTP
 group-object LWAPP
 group-object CAPWAP
object-group service TCP1080
 service-object tcp destination eq 1080
object-group service TCP8080
 service-object tcp destination eq 8080
object-group service RDP
 description Windows Remote Desktop
 service-object tcp destination eq 3389
object-group service CSM_INLINE_svc_rule_77309411645
 description Generated by CS-Manager from service of FirewallRule# 11
(ASA-DC-1-vdc1_v1/mandatory)
 service-object icmp echo
 service-object icmp echo-reply
 service-object tcp destination eq www
 service-object tcp destination eq https
 service-object tcp destination eq ssh
 service-object tcp destination eq ftp
 group-object HTTPS-8443
 group-object TCP1080
 group-object TCP8080
 group-object RDP
object-group service CISCO-WAAS
 description Ports for Cisco WAAS
 service-object tcp destination eq 4050
object-group service Netbios
 description Netbios Servers
 service-object udp destination eq netbios-dgm
```

```
 service-object udp destination eq netbios-ns
 service-object tcp destination eq netbios-ssn
object-group service CSM_INLINE_svc_rule_77309411647
 description Generated by CS-Manager from service of FirewallRule# 12
(ASA-DC-1-vdc1_v1/mandatory)
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Microsoft-DS-SMB
 group-object Netbios
object-group service CSM_INLINE_svc_rule_77309411649
 description Generated by CS-Manager from service of FirewallRule# 13
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp-udp destination eq sip
 service-object tcp destination eq 2000
object-group service CSM_INLINE_svc_rule_77309414071
 description Generated by CS-Manager from service of FirewallRule# 15
(ASA-DC-1-vdc1_v1/mandatory)
 service-object icmp echo
 service-object icmp echo-reply
 service-object icmp unreachable
 service-object tcp destination eq www
 service-object tcp destination eq https
 service-object tcp destination eq ftp
 service-object tcp destination eq ssh
 group-object TCP1080
 group-object TCP8080
 group-object RDP
object-group service NTP
 description NTP Protocols
 service-object tcp destination eq 123
 service-object udp destination eq ntp
object-group service CSM_INLINE_svc_rule_77309414073
 description Generated by CS-Manager from service of FirewallRule# 16
(ASA-DC-1-vdc1_v1/mandatory)
 group-object DNS-Resolving
 group-object NTP
object-group service CSM_INLINE_svc_rule_77309414077
 description Generated by CS-Manager from service of FirewallRule# 18
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp destination eq ldap
 service-object tcp destination eq ldaps
 group-object LDAP-GC
 group-object LDAP-GC-SSL
 group-object LDAP-UDP
object-group service CSM_INLINE_svc_rule_77309411655
 description Generated by CS-Manager from service of FirewallRule# 21
(ASA-DC-1-vdc1_v1/mandatory)
 service-object udp destination eq snmptrap
 service-object udp destination eq snmp
 service-object udp destination eq syslog
object-group service CSM_INLINE_svc_rule_77309411657
 description Generated by CS-Manager from service of FirewallRule# 22
(ASA-DC-1-vdc1_v1/mandatory)
 service-object udp destination eq domain
 service-object tcp destination eq ldap
 service-object tcp destination eq ldaps
object-group service CSM_INLINE_svc_rule_77309411663
 description Generated by CS-Manager from service of FirewallRule# 25
(ASA-DC-1-vdc1_v1/mandatory)
 service-object udp destination eq 1812
 service-object udp destination eq 1813
object-group service CSM_INLINE_svc_rule_77309411665
 description Generated by CS-Manager from service of FirewallRule# 26
(ASA-DC-1-vdc1_v1/mandatory)
```

```
 service-object tcp destination eq https
 service-object tcp destination eq www
 group-object HTTPS-8443
object-group service ESX-SLP
 description CIM Service Location Protocol (SLP) for VMware systems
 service-object udp destination eq 427
 service-object tcp destination eq 427
object-group service CSM_INLINE_svc_rule_77309411667
 description Generated by CS-Manager from service of FirewallRule# 27
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp destination eq https
 service-object tcp destination eq www
 service-object tcp destination eq ssh
 group-object vCenter-to-ESX4
 group-object ESX-SLP
object-group service Cisco-Mobility
 description Mobility ports for Wireless
 service-object udp destination eq 16666
 service-object udp destination eq 16667
object-group service CSM_INLINE_svc_rule_77309411671
 description Generated by CS-Manager from service of FirewallRule# 29
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp destination eq https
 service-object udp destination eq isakmp
 group-object Cisco-Mobility
 group-object IP-Protocol-97
 group-object LWAPP
 group-object CAPWAP
object-group service CSM_INLINE_svc_rule_77309411673
 description Generated by CS-Manager from service of FirewallRule# 30
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp-udp destination eq sip
 service-object tcp destination eq 2000
object-group service CSM_INLINE_svc_rule_77309411675
 description Generated by CS-Manager from service of FirewallRule# 31
(ASA-DC-1-vdc1_v1/mandatory)
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Microsoft-DS-SMB
 group-object Netbios
object-group service CSM_INLINE_svc_rule_77309411677
 description Generated by CS-Manager from service of FirewallRule# 32
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp destination eq ldap
 service-object tcp destination eq ldaps
 service-object udp destination eq 88
 service-object udp destination eq ntp
 service-object udp destination eq netbios-dgm
 group-object RPC
 group-object LDAP-GC
 group-object LDAP-GC-SSL
 group-object DNS-Resolving
 group-object Kerberos-TCP
 group-object Microsoft-DS-SMB
 group-object LDAP-UDP
 group-object RPC-HighPorts
object-group service CSM_INLINE_svc_rule_77309411679
 description Generated by CS-Manager from service of FirewallRule# 33
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp destination eq www
 service-object tcp destination eq https
object-group service CSM_INLINE_svc_rule_77309411681
 description Generated by CS-Manager from service of FirewallRule# 34
(ASA-DC-1-vdc1_v1/mandatory)
```

```
 service-object tcp destination eq www
 service-object tcp destination eq https
 service-object tcp destination eq smtp
 service-object tcp destination eq pop3
 service-object tcp destination eq imap4
object-group service CSM_INLINE_svc_rule_77309414166
 description Generated by CS-Manager from service of FirewallRule# 40
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp destination eq smtp
 group-object DNS-Resolving
object-group service CSM_INLINE_svc_rule_77309414172
 description Generated by CS-Manager from service of FirewallRule# 43
(ASA-DC-1-vdc1_v1/mandatory)
 service-object udp destination eq 1812
 service-object udp destination eq 1813
object-group service CSM_INLINE_svc_rule_77309414176
 description Generated by CS-Manager from service of FirewallRule# 45
(ASA-DC-1-vdc1_v1/mandatory)
 service-object icmp
 service-object tcp destination eq ssh
 service-object tcp destination eq telnet
 service-object tcp destination eq www
 service-object tcp destination eq https
 service-object tcp destination eq 8880
 service-object tcp destination eq 8444
 service-object tcp destination eq 5900
 service-object tcp destination eq 5800
 group-object RDP
 group-object TCP1080
 group-object TCP8080
 group-object TFTP
 group-object HTTPS-8443
 group-object vCenter-to-ESX4
access-list CSM_FW_ACL_north extended permit ospf 192.168.162.0 255.255.255.0
192.168.162.0 255.255.255.0
access-list CSM_FW_ACL_north extended permit tcp object-group Branches-ALL object-group
EMC-NCM eq ssh
access-list CSM_FW_ACL_north extended permit object-group CSM_INLINE_svc_rule_77309411655
object-group Branches-ALL object-group RSA-enVision
access-list CSM_FW_ACL_north extended permit object-group CSM_INLINE_svc_rule_77309411657
object-group Branches-ALL object-group ActiveDirectory.cisco-irn.com
access-list CSM_FW_ACL_north extended permit tcp object-group Branches-ALL object-group
TACACS eq tacacs
access-list CSM_FW_ACL_north extended permit udp object-group Branches-ALL object-group
NTP-Servers eq ntp
access-list CSM_FW_ACL_north extended permit object-group CSM_INLINE_svc_rule_77309411663
object-group Branches-ALL object-group CSM_INLINE_dst_rule_77309411663
access-list CSM_FW_ACL_north extended permit object-group CSM_INLINE_svc_rule_77309411665
object-group Branches-ALL object-group CSM_INLINE_dst_rule_77309411665
access-list CSM_FW_ACL_north remark VMWare ESX to Data Center
access-list CSM_FW_ACL_north extended permit object-group CSM_INLINE_svc_rule_77309411667
object-group Branches-ALL object-group vSphere-1
access-list CSM_FW_ACL_north remark Physical security systems
access-list CSM_FW_ACL_north extended permit tcp object-group Branches-ALL object-group
CSM_INLINE_dst_rule_77309411669 eq https
access-list CSM_FW_ACL_north remark Wireless control systems
access-list CSM_FW_ACL_north extended permit object-group CSM_INLINE_svc_rule_77309411671
object-group Branches-ALL object-group CSM_INLINE_dst_rule_77309411671
access-list CSM_FW_ACL_north remark Voice calls
access-list CSM_FW_ACL_north extended permit object-group CSM_INLINE_svc_rule_77309411673
object-group Branches-ALL object-group DC-ALL
access-list CSM_FW_ACL_north remark WAAS systems
access-list CSM_FW_ACL_north extended permit object-group CSM_INLINE_svc_rule_77309411675
object-group Branches-ALL object-group DC-WAAS
```

```
access-list CSM_FW_ACL_north remark Allow Active Directory Domain
access-list CSM_FW_ACL_north extended permit object-group CSM_INLINE_svc_rule_77309411677
object-group Branches-ALL object-group ActiveDirectory.cisco-irn.com
access-list CSM_FW_ACL_north remark Allow Windows Updates
access-list CSM_FW_ACL_north extended permit object-group CSM_INLINE_svc_rule_77309411679
object-group Branches-ALL object-group MS-Update
access-list CSM_FW_ACL_north remark Allow Mail
access-list CSM_FW_ACL_north extended permit object-group CSM_INLINE_svc_rule_77309411681
object-group Branches-ALL object-group MSExchange
access-list CSM_FW_ACL_north remark Allow Applications
access-list CSM_FW_ACL_north extended permit tcp object-group
CSM_INLINE_src_rule_77309411683 object-group CSM_INLINE_dst_rule_77309411683 eq https
access-list CSM_FW_ACL_north extended permit udp object-group
CSM_INLINE_src_rule_77309414158 object-group NTP-Servers eq ntp
access-list CSM_FW_ACL_north remark - RIE-2
access-list CSM_FW_ACL_north extended permit udp object-group
CSM_INLINE_src_rule_77309414160 object-group RSA-enVision eq syslog
access-list CSM_FW_ACL_north extended permit tcp object-group
CSM_INLINE_src_rule_77309414162 object-group TACACS eq tacacs
access-list CSM_FW_ACL_north extended permit udp 192.168.21.0 255.255.255.0 object-group
ActiveDirectory.cisco-irn.com eq domain
access-list CSM_FW_ACL_north remark Ironport traffic in from DNZ
access-list CSM_FW_ACL_north extended permit object-group CSM_INLINE_svc_rule_77309414166
host 192.168.23.68 any
access-list CSM_FW_ACL_north extended permit udp host 192.168.23.68 object-group
RSA-enVision eq syslog
access-list CSM_FW_ACL_north extended permit udp host 192.168.23.68 object-group
NTP-Servers eq ntp
access-list CSM_FW_ACL_north extended permit object-group CSM_INLINE_svc_rule_77309414172
host 192.168.23.68 object-group TACACS
access-list CSM_FW_ACL_north remark Drop all other traffic
access-list CSM_FW_ACL_north extended deny ip any any log
access-list CSM_FW_ACL_south extended permit ospf 192.168.162.0 255.255.255.0
192.168.162.0 255.255.255.0
access-list CSM_FW_ACL_south extended permit ip object-group
CSM_INLINE_src_rule_77309411633 object-group CSM_INLINE_dst_rule_77309411633
access-list CSM_FW_ACL_south extended permit object-group CSM_INLINE_svc_rule_77309411635
object-group Admin-Systems object-group CSM_INLINE_dst_rule_77309411635
access-list CSM_FW_ACL_south remark Allow services for Ironport apps
access-list CSM_FW_ACL_south extended permit object-group CSM_INLINE_svc_rule_77309414079
object-group CSM_INLINE_src_rule_77309414079 192.168.23.64 255.255.255.224
access-list CSM_FW_ACL_south remark Allow traffic to DMZ
access-list CSM_FW_ACL_south extended permit object-group CSM_INLINE_svc_rule_77309414081
object-group CSM_INLINE_src_rule_77309414081 host 192.168.20.30
access-list CSM_FW_ACL_south remark Drop unauthorized traffic to DMZ
access-list CSM_FW_ACL_south extended deny ip any 192.168.20.0 255.255.252.0 log
access-list CSM_FW_ACL_south remark Allow Active Directory Domain
access-list CSM_FW_ACL_south extended permit object-group CSM_INLINE_svc_rule_77309411637
object-group ActiveDirectory.cisco-irn.com object-group Branches-ALL
access-list CSM_FW_ACL_south remark VMWare - ESX systems
access-list CSM_FW_ACL_south extended permit object-group CSM_INLINE_svc_rule_77309411639
object-group vSphere-1 object-group Branches-ALL
access-list CSM_FW_ACL_south remark Wireless Management to Stores
access-list CSM_FW_ACL_south extended permit object-group CSM_INLINE_svc_rule_77309411641
object-group CSM_INLINE_src_rule_77309411641 object-group Branches-ALL
access-list CSM_FW_ACL_south remark Physical security systems
access-list CSM_FW_ACL_south extended permit tcp object-group
CSM_INLINE_src_rule_77309411643 object-group Branches-ALL eq https
access-list CSM_FW_ACL_south remark Allow Management of branch systems
access-list CSM_FW_ACL_south extended permit object-group CSM_INLINE_svc_rule_77309411645
object-group DC-ALL object-group Branches-ALL
access-list CSM_FW_ACL_south remark WAAS systems
access-list CSM_FW_ACL_south extended permit object-group CSM_INLINE_svc_rule_77309411647
object-group DC-WAAS object-group Branches-ALL
```

```
access-list CSM_FW_ACL_south remark Voice calls
access-list CSM_FW_ACL_south extended permit object-group CSM_INLINE_svc_rule_77309411649
object-group DC-ALL object-group Branches-ALL
access-list CSM_FW_ACL_south extended deny ip any object-group Branches-ALL
access-list CSM_FW_ACL_south remark Allow outbound services for Internet
access-list CSM_FW_ACL_south extended permit object-group CSM_INLINE_svc_rule_77309414071
object-group CSM_INLINE_src_rule_77309414071 any
access-list CSM_FW_ACL_south extended permit object-group CSM_INLINE_svc_rule_77309414073
object-group ActiveDirectory.cisco-irn.com any
access-list CSM_FW_ACL_south extended permit udp object-group NTP-Servers any eq ntp
access-list CSM_FW_ACL_south remark Allow LDAP out LAB test
access-list CSM_FW_ACL_south extended permit object-group CSM_INLINE_svc_rule_77309414077
object-group PAME-DC-1 any log
access-list CSM_FW_ACL_south remark Drop and Log all other traffic
access-list CSM_FW_ACL_south extended deny ip any any log
pager lines 24
logging host south 192.168.42.124
mtu north 1500
mtu south 1500
icmp unreachable rate-limit 1 burst-size 1
icmp permit any north
icmp permit any south
asdm history enable
arp timeout 14400
access-group CSM_FW_ACL_north in interface north
access-group CSM_FW_ACL_south in interface south
route north 0.0.0.0 0.0.0.0 192.168.162.1 1
route south 192.168.38.0 255.255.255.0 192.168.162.7 1
route south 192.168.39.0 255.255.255.0 192.168.162.7 1
route south 192.168.40.0 255.255.255.0 192.168.162.7 1
route south 192.168.41.0 255.255.255.0 192.168.162.7 1
route south 192.168.42.0 255.255.255.0 192.168.162.7 1
route south 192.168.43.0 255.255.255.0 192.168.162.7 1
route south 192.168.44.0 255.255.255.0 192.168.162.7 1
route south 192.168.45.0 255.255.255.0 192.168.162.7 1
route south 192.168.46.0 255.255.255.0 192.168.162.7 1
route south 192.168.52.0 255.255.255.0 192.168.162.7 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
aaa-server CiscoACS protocol tacacs+
aaa-server CiscoACS (south) host 192.168.42.131
 key *****
aaa authentication ssh console CiscoACS LOCAL
aaa authentication enable console CiscoACS LOCAL
aaa authentication http console CiscoACS LOCAL
aaa accounting ssh console CiscoACS
aaa accounting enable console CiscoACS
aaa accounting command privilege 15 CiscoACS
aaa authentication secure-http-client
aaa local authentication attempts max-fail 6
aaa authorization exec authentication-server
http server enable
http server idle-timeout 15
http server session-timeout 60
http 10.19.151.99 255.255.255.255 north
http 192.168.41.101 255.255.255.255 south
http 192.168.41.102 255.255.255.255 south
http 192.168.42.122 255.255.255.255 south
http 192.168.42.124 255.255.255.255 south
http 192.168.42.133 255.255.255.255 south
```

```
http 192.168.42.138 255.255.255.255 south
no snmp-server location
no snmp-server contact
telnet timeout 5
ssh 10.19.151.99 255.255.255.255 north
ssh 192.168.41.101 255.255.255.255 south
ssh 192.168.41.102 255.255.255.255 south
ssh 192.168.42.122 255.255.255.255 south
ssh 192.168.42.124 255.255.255.255 south
ssh 192.168.42.133 255.255.255.255 south
ssh 192.168.42.138 255.255.255.255 south
ssh timeout 15
ssh version 2
no threat-detection statistics tcp-intercept
username csmadmin password  <removed> encrypted privilege 15
username bmcgloth password <removed> encrypted privilege 15
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:70afa3a2a3007db41f3f336aca5cf51d
: end
asdm history enable
```

RAGG-1-RUNNING

```
version 5.1(2)
hostname RAGG-1
vdc RAGG-1 id 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource monitor-session minimum 0 maximum 2
  limit-resource monitor-session-erspan-dst minimum 0 maximum 23
  limit-resource vrf minimum 2 maximum 1000
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 32 maximum 32
  limit-resource u6route-mem minimum 16 maximum 16
```

```
  limit-resource m4route-mem minimum 48 maximum 48
  limit-resource m6route-mem minimum 8 maximum 8
vdc vdc1 id 2
  allocate interface Ethernet1/1,Ethernet1/3,Ethernet1/5,Ethernet1/7,Ethernet1/25-32
  allocate interface Ethernet2/1-12
  boot-order 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource monitor-session minimum 0 maximum 2
  limit-resource monitor-session-erspan-dst minimum 0 maximum 23
  limit-resource vrf minimum 2 maximum 1000
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 8 maximum 8
  limit-resource u6route-mem minimum 4 maximum 4
  limit-resource m4route-mem minimum 8 maximum 8
  limit-resource m6route-mem minimum 5 maximum 5
vdc vdc2 id 3
  allocate interface Ethernet1/2,Ethernet1/4,Ethernet1/6,Ethernet1/8-24
  allocate interface Ethernet2/13-48
  boot-order 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource monitor-session minimum 0 maximum 2
  limit-resource monitor-session-erspan-dst minimum 0 maximum 23
  limit-resource vrf minimum 2 maximum 1000
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 8 maximum 8
  limit-resource u6route-mem minimum 4 maximum 4
  limit-resource m4route-mem minimum 8 maximum 8
  limit-resource m6route-mem minimum 5 maximum 5

feature privilege
feature tacacs+

username bart password 5 <removed> role network-admin
username emc-ncm password 5 <removed>  role network-admin
enable secret 5 <removed>

banner motd @
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                  **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
@

ssh login-attempts 6

ip domain-lookup
ip domain-name cisco-irn.com
ip host RAGG-1 192.168.42.36
tacacs-server key 7 "<removed>"
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
    use-vrf management
ip access-list 23
  statistics per-entry
```

```
  10 permit ip 127.0.0.1/32 192.168.42.36/32
  20 permit ip 192.168.41.101/32 192.168.42.36/32
  30 permit ip 192.168.41.102/32 192.168.42.36/32
  40 permit ip 192.168.42.111/32 192.168.42.36/32
  50 permit ip 192.168.42.122/32 192.168.42.36/32
  60 permit ip 192.168.42.131/32 192.168.42.36/32
  70 permit ip 192.168.42.133/32 192.168.42.36/32
  80 permit ip 192.168.42.138/32 192.168.42.36/32
  90 permit ip 10.19.151.99/32 192.168.42.36/32
  100 deny ip any any
ip access-list 88
  statistics per-entry
  10 permit ip 192.168.42.122/32 192.168.42.36/32
  20 deny ip any any
ip access-list copp-system-acl-bgp
  10 permit tcp any gt 1024 any eq bgp
  20 permit tcp any eq bgp any gt 1024
ipv6 access-list copp-system-acl-bgp6
  10 permit tcp any gt 1024 any eq bgp
  20 permit tcp any eq bgp any gt 1024
ip access-list copp-system-acl-eigrp
  10 permit eigrp any any
ip access-list copp-system-acl-ftp
  10 permit tcp any any eq ftp-data
  20 permit tcp any any eq ftp
  30 permit tcp any eq ftp-data any
  40 permit tcp any eq ftp any
ip access-list copp-system-acl-glbp
  10 permit udp any eq 3222 224.0.0.0/24 eq 3222
ip access-list copp-system-acl-hsrp
  10 permit udp any 224.0.0.0/24 eq 1985
ip access-list copp-system-acl-icmp
  10 permit icmp any any echo
  20 permit icmp any any echo-reply
ipv6 access-list copp-system-acl-icmp6
  10 permit icmp any any echo-request
  20 permit icmp any any echo-reply
ipv6 access-list copp-system-acl-icmp6-msgs
  10 permit icmp any any router-advertisement
  20 permit icmp any any router-solicitation
  30 permit icmp any any nd-na
  40 permit icmp any any nd-ns
  50 permit icmp any any mld-query
  60 permit icmp any any mld-report
  70 permit icmp any any mld-reduction
ip access-list copp-system-acl-igmp
  10 permit igmp any 224.0.0.0/3
ip access-list copp-system-acl-msdp
  10 permit tcp any gt 1024 any eq 639
  20 permit tcp any eq 639 any gt 1024
ip access-list copp-system-acl-ntp
  10 permit udp any any eq ntp
  20 permit udp any eq ntp any
ipv6 access-list copp-system-acl-ntp6
  10 permit udp any any eq ntp
  20 permit udp any eq ntp any
ip access-list copp-system-acl-ospf
  10 permit ospf any any
ipv6 access-list copp-system-acl-ospf6
  10 permit 89 any any
ip access-list copp-system-acl-pim
  10 permit pim any 224.0.0.0/24
  20 permit udp any any eq pim-auto-rp
ip access-list copp-system-acl-pim-reg
```

```
  10 permit pim any any
ipv6 access-list copp-system-acl-pim6
  10 permit 103 any ff02::d/128
  20 permit udp any any eq pim-auto-rp
ip access-list copp-system-acl-radius
  10 permit udp any any eq 1812
  20 permit udp any any eq 1813
  30 permit udp any any eq 1645
  40 permit udp any any eq 1646
  50 permit udp any eq 1812 any
  60 permit udp any eq 1813 any
  70 permit udp any eq 1645 any
  80 permit udp any eq 1646 any
ipv6 access-list copp-system-acl-radius6
  10 permit udp any any eq 1812
  20 permit udp any any eq 1813
  30 permit udp any any eq 1645
  40 permit udp any any eq 1646
  50 permit udp any eq 1812 any
  60 permit udp any eq 1813 any
  70 permit udp any eq 1645 any
  80 permit udp any eq 1646 any
ip access-list copp-system-acl-rip
  10 permit udp any 224.0.0.0/24 eq rip
ip access-list copp-system-acl-sftp
  10 permit tcp any any eq 115
  20 permit tcp any eq 115 any
ip access-list copp-system-acl-snmp
  10 permit udp any any eq snmp
  20 permit udp any any eq snmptrap
ip access-list copp-system-acl-ssh
  10 permit tcp any any eq 22
  20 permit tcp any eq 22 any
ipv6 access-list copp-system-acl-ssh6
  10 permit tcp any any eq 22
  20 permit tcp any eq 22 any
ip access-list copp-system-acl-tacacs
  10 permit tcp any any eq tacacs
  20 permit tcp any eq tacacs any
ipv6 access-list copp-system-acl-tacacs6
  10 permit tcp any any eq tacacs
  20 permit tcp any eq tacacs any
ip access-list copp-system-acl-telnet
  10 permit tcp any any eq telnet
  20 permit tcp any any eq 107
  30 permit tcp any eq telnet any
  40 permit tcp any eq 107 any
ipv6 access-list copp-system-acl-telnet6
  10 permit tcp any any eq telnet
  20 permit tcp any any eq 107
  30 permit tcp any eq telnet any
  40 permit tcp any eq 107 any
ip access-list copp-system-acl-tftp
  10 permit udp any any eq tftp
  20 permit udp any any eq 1758
  30 permit udp any eq tftp any
  40 permit udp any eq 1758 any
ipv6 access-list copp-system-acl-tftp6
  10 permit udp any any eq tftp
  20 permit udp any any eq 1758
  30 permit udp any eq tftp any
  40 permit udp any eq 1758 any
ip access-list copp-system-acl-traceroute
  10 permit icmp any any ttl-exceeded
```

```
  20 permit icmp any any port-unreachable
ip access-list copp-system-acl-undesirable
  10 permit udp any any eq 1434
ip access-list copp-system-acl-vpc
  10 permit udp any any eq 3200
ip access-list copp-system-acl-vrrp
  10 permit 112 any 224.0.0.0/24
class-map type control-plane match-any copp-system-class-critical
  match access-group name copp-system-acl-bgp
  match access-group name copp-system-acl-bgp6
  match access-group name copp-system-acl-eigrp
  match access-group name copp-system-acl-igmp
  match access-group name copp-system-acl-msdp
  match access-group name copp-system-acl-ospf
  match access-group name copp-system-acl-ospf6
  match access-group name copp-system-acl-pim
  match access-group name copp-system-acl-pim6
  match access-group name copp-system-acl-rip
  match access-group name copp-system-acl-vpc
class-map type control-plane match-any copp-system-class-exception
  match exception ip option
  match exception ip icmp unreachable
  match exception ipv6 option
  match exception ipv6 icmp unreachable
class-map type control-plane match-any copp-system-class-important
  match access-group name copp-system-acl-glbp
  match access-group name copp-system-acl-hsrp
  match access-group name copp-system-acl-vrrp
  match access-group name copp-system-acl-icmp6-msgs
  match access-group name copp-system-acl-pim-reg
class-map type control-plane match-any copp-system-class-management
  match access-group name copp-system-acl-ftp
  match access-group name copp-system-acl-ntp
  match access-group name copp-system-acl-ntp6
  match access-group name copp-system-acl-radius
  match access-group name copp-system-acl-sftp
  match access-group name copp-system-acl-snmp
  match access-group name copp-system-acl-ssh
  match access-group name copp-system-acl-ssh6
  match access-group name copp-system-acl-tacacs
  match access-group name copp-system-acl-telnet
  match access-group name copp-system-acl-tftp
  match access-group name copp-system-acl-tftp6
  match access-group name copp-system-acl-radius6
  match access-group name copp-system-acl-tacacs6
  match access-group name copp-system-acl-telnet6
class-map type control-plane match-any copp-system-class-monitoring
  match access-group name copp-system-acl-icmp
  match access-group name copp-system-acl-icmp6
  match access-group name copp-system-acl-traceroute
class-map type control-plane match-any copp-system-class-normal
  match protocol arp
class-map type control-plane match-any copp-system-class-redirect
  match redirect dhcp-snoop
  match redirect arp-inspect
class-map type control-plane match-any copp-system-class-undesirable
  match access-group name copp-system-acl-undesirable
policy-map type control-plane copp-system-policy
  class copp-system-class-critical
    police cir 39600 kbps bc 250 ms conform transmit violate drop
  class copp-system-class-important
    police cir 1060 kbps bc 1000 ms conform transmit violate drop
  class copp-system-class-management
    police cir 10000 kbps bc 250 ms conform transmit violate drop
```

```
  class copp-system-class-normal
    police cir 680 kbps bc 250 ms conform transmit violate drop
  class copp-system-class-redirect
    police cir 280 kbps bc 250 ms conform transmit violate drop
  class copp-system-class-monitoring
    police cir 130 kbps bc 1000 ms conform transmit violate drop
  class copp-system-class-exception
    police cir 360 kbps bc 250 ms conform transmit violate drop
  class copp-system-class-undesirable
    police cir 32 kbps bc 250 ms conform drop violate drop
  class class-default
    police cir 100 kbps bc 250 ms conform transmit violate drop
control-plane
  service-policy input copp-system-policy
snmp-server user bart network-admin auth md5 <removed> priv <removed> localizedkey
snmp-server user bmcgloth network-admin auth md5 <removed> priv <removed> localizedkey
ntp server 192.168.62.161 use-vrf management
ntp server 192.168.62.162 use-vrf management
aaa authentication login default group CiscoACS
aaa authentication login console group CiscoACS
aaa authorization ssh-certificate default group CiscoACS
aaa accounting default group CiscoACS
aaa authentication login error-enable

vrf context management
  ip route 0.0.0.0/0 192.168.42.1
vlan 1

interface mgmt0
  ip address 192.168.42.36/24
clock timezone PST -8 0
clock summer-time PST 1 Sun April 02:00 5 Sun Oct 02:00 60
  logout-warning 20
line console
  exec-timeout 15
line vty
  exec-timeout 15
  access-class 23 in
boot kickstart bootflash:/n7000-s1-kickstart.5.1.2.bin sup-1
boot system bootflash:/n7000-s1-dk9.5.1.2.bin sup-1
boot kickstart bootflash:/n7000-s1-kickstart.5.1.2.bin sup-2
boot system bootflash:/n7000-s1-dk9.5.1.2.bin sup-2
logging server 192.168.42.124 6 use-vrf management
```

RAGG-1-VDC1-RUNNING

```
version 5.1(2)
hostname vdc1

feature privilege
feature tacacs+
cfs eth distribute
feature ospf
feature pim
feature udld
feature interface-vlan
feature hsrp
feature lacp
feature glbp
```

```
feature vpc

username bmcgloth password 5 <removed> role vdc-admin
username bart password 5 <removed>  role vdc-admin
enable secret 5 <removed>

banner motd @
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                  **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
@

ssh login-attempts 6

ip domain-lookup
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
tacacs-server key 7 "<removed>"
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
    source-interface loopback0
ip access-list 23
  statistics per-entry
  10 permit ip 127.0.0.1/32 192.168.1.11/32
  20 permit ip 192.168.41.101/32 192.168.1.11/32
  30 permit ip 192.168.41.102/32 192.168.1.11/32
  40 permit ip 192.168.42.111/32 192.168.1.11/32
  50 permit ip 192.168.42.122/32 192.168.1.11/32
  60 permit ip 192.168.42.131/32 192.168.1.11/32
  70 permit ip 192.168.42.133/32 192.168.1.11/32
  80 permit ip 192.168.42.138/32 192.168.1.11/32
  90 permit ip 10.19.151.99/32 192.168.1.11/32
  100 deny ip any any
ip access-list 88
  statistics per-entry
  10 permit ip 192.168.42.122/32 192.168.1.11/32
  20 deny ip any any
snmp-server source-interface trap loopback0
snmp-server source-interface inform loopback0
snmp-server user bart vdc-admin auth md5 <removed> priv <removed> localizedkey
snmp-server user bmcgloth vdc-admin auth md5 <removed> priv <removed> localizedkey
no snmp-server enable traps entity entity_mib_change
no snmp-server enable traps entity entity_module_status_change
no snmp-server enable traps entity entity_power_status_change
no snmp-server enable traps entity entity_module_inserted
no snmp-server enable traps entity entity_module_removed
no snmp-server enable traps entity entity_unrecognised_module
no snmp-server enable traps entity entity_fan_status_change
no snmp-server enable traps entity entity_power_out_change
no snmp-server enable traps link linkDown
no snmp-server enable traps link linkUp
no snmp-server enable traps link IETF-extended-linkDown
no snmp-server enable traps link IETF-extended-linkUp
```

```
no snmp-server enable traps link cisco-extended-linkDown
no snmp-server enable traps link cisco-extended-linkUp
snmp-server enable traps callhome event-notify
snmp-server enable traps callhome smtp-send-fail
snmp-server enable traps cfs state-change-notif
snmp-server enable traps cfs merge-failure
no snmp-server enable traps rf redundancy_framework
snmp-server enable traps aaa server-state-change
no snmp-server enable traps license notify-license-expiry
no snmp-server enable traps license notify-no-license-for-feature
no snmp-server enable traps license notify-licensefile-missing
no snmp-server enable traps license notify-license-expiry-warning
snmp-server enable traps hsrp state-change
no snmp-server enable traps upgrade UpgradeOpNotifyOnCompletion
no snmp-server enable traps upgrade UpgradeJobStatusNotify
snmp-server enable traps feature-control FeatureOpStatusChange
snmp-server enable traps link cisco-xcvr-mon-status-chg
snmp-server enable traps vtp notifs
snmp-server enable traps vtp vlancreate
snmp-server enable traps vtp vlandelete
snmp-server enable traps bridge newroot
snmp-server enable traps bridge topologychange
snmp-server enable traps stpx inconsistency
snmp-server enable traps stpx root-inconsistency
snmp-server enable traps stpx loop-inconsistency
aaa authentication login default group CiscoACS
aaa authorization ssh-certificate default group CiscoACS
aaa accounting default group CiscoACS
aaa authentication login error-enable

vrf context management
vlan 1,3,151,161

interface Vlan1

interface Vlan3
  no shutdown
  ip address 192.168.10.61/30
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 3 <removed>
  ip ospf dead-interval 3
  ip ospf hello-interval 1
  ip router ospf 5 area 0.0.0.0

interface Vlan151
  no shutdown
  ip address 192.168.152.3/24
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 3 <removed>
  ip ospf priority 3
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 1
    authentication text c1sc0
    preempt delay minimum 180
    priority 10 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.152.1

interface Vlan161
  no shutdown
  ip address 192.168.162.3/24
  ip ospf authentication message-digest
```

```
  ip ospf message-digest-key 1 md5 3 <removed>
  ip ospf priority 5
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 1
    authentication text c1sc0
    preempt delay minimum 180
    priority 10 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.162.1

interface port-channel99
  switchport
  switchport mode trunk
  spanning-tree port type network

interface Ethernet1/1
  description 10Gig LINK to RCORE-1 T2/1
  no switchport
  logging event port link-status
  no ip redirects
  ip address 192.168.10.14/30
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 3 <removed>
  ip ospf dead-interval 6
  ip ospf hello-interval 2
  ip ospf network point-to-point
  ip router ospf 5 area 0.0.0.0
  ip pim sparse-mode
  ip igmp version 3
  no shutdown

interface Ethernet1/3
  description 10Gig LINK to RCORE-2 T2/1
  no switchport
  logging event port link-status
  no ip redirects
  ip address 192.168.10.22/30
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 3 <removed>
  ip ospf dead-interval 6
  ip ospf hello-interval 2
  ip ospf network point-to-point
  ip router ospf 5 area 0.0.0.0
  ip pim sparse-mode
  ip igmp version 3
  no shutdown

interface Ethernet1/5
  description to DC-ASA-1 vc1 T0/6
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 161
  spanning-tree port type normal
  no shutdown

interface Ethernet1/7
  description to DC-ASA-1 vc2 T0/8
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 151
  spanning-tree port type normal
  no shutdown
```

```
interface Ethernet1/25
  no switchport

interface Ethernet1/26
  no switchport

interface Ethernet1/27
  no switchport

interface Ethernet1/28
  no switchport

interface Ethernet1/29
  description RAGG-2 vPC Channel link
  switchport
  switchport mode trunk
  channel-group 99 mode active
  no shutdown

interface Ethernet1/30
  description RAGG-2 vPC Channel link
  switchport
  switchport mode trunk
  channel-group 99 mode active
  no shutdown

interface Ethernet1/31
  description RAGG-2 vPC Channel link
  switchport
  switchport mode trunk
  channel-group 99 mode active
  no shutdown

interface Ethernet1/32
  description RAGG-2 vPC Channel link
  switchport
  switchport mode trunk
  channel-group 99 mode active
  no shutdown

interface Ethernet2/1
  no switchport

interface Ethernet2/2
  no switchport

interface Ethernet2/3
  no switchport

interface Ethernet2/4
  no switchport

interface Ethernet2/5
  no switchport

interface Ethernet2/6
  no switchport

interface Ethernet2/7
  no switchport

interface Ethernet2/8
  no switchport
```

```
interface Ethernet2/9
  no switchport

interface Ethernet2/10
  no switchport

interface Ethernet2/11
  no switchport

interface Ethernet2/12
  no switchport

interface loopback0
  ip address 192.168.1.11/32
  ip router ospf 5 area 0.0.0.0
logging server 192.168.42.124 6
logging source-interface loopback 0
  logout-warning 20
line console
  exec-timeout 15
line vty
  exec-timeout 15
  access-class 23 in
router ospf 5
  router-id 192.168.1.11
  area 0.0.0.81 nssa
  area 0.0.0.0 range 192.168.1.11/32
  area 0.0.0.0 range 192.168.10.12/30
  area 0.0.0.0 range 192.168.10.20/30
  area 0.0.0.0 range 192.168.10.60/30
  area 0.0.0.81 range 192.168.152.0/24
  area 0.0.0.81 range 192.168.162.0/24
  area 0.0.0.0 authentication message-digest
  area 0.0.0.81 authentication message-digest
  timers throttle spf 10 100 5000
  auto-cost reference-bandwidth 10000
ip pim ssm range 232.0.0.0/8
```

RAGG-1-VDC2-RUNNING

```
version 5.1(2)
hostname vdc2

feature privilege
feature tacacs+
cfs eth distribute
feature ospf
feature pim
feature udld
feature interface-vlan
feature hsrp
feature lacp
feature vpc

username bart password 5 <removed>   role vdc-admin
username bmcgloth password 5 <removed> role vdc-admin
enable secret 5 <removed>

banner motd @
```

```
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
@

ssh login-attempts 6

ip domain-lookup
ip domain-name cisco-irn.com
tacacs-server key 7 "<removed>"
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
    use-vrf servers1
    source-interface loopback0
ip access-list 23
  statistics per-entry
  10 permit ip 127.0.0.1/32 192.168.1.31/32
  20 permit ip 192.168.41.101/32 192.168.1.31/32
  30 permit ip 192.168.41.102/32 192.168.1.31/32
  40 permit ip 192.168.42.111/32 192.168.1.31/32
  50 permit ip 192.168.42.122/32 192.168.1.31/32
  60 permit ip 192.168.42.131/32 192.168.1.31/32
  70 permit ip 192.168.42.133/32 192.168.1.31/32
  80 permit ip 192.168.42.138/32 192.168.1.31/32
  90 permit ip 10.19.151.99/32 192.168.1.31/32
  100 deny ip any any
ip access-list 88
  statistics per-entry
  10 permit ip 192.168.42.122/32 192.168.1.31/32
  20 deny ip any any
snmp-server source-interface trap loopback0
snmp-server source-interface inform loopback0
snmp-server user bart vdc-admin auth md5 <removed> priv <removed> localizedkey
snmp-server user bmcgloth vdc-admin auth md5 <removed> priv <removed> localizedkey
no snmp-server enable traps entity entity_mib_change
no snmp-server enable traps entity entity_module_status_change
no snmp-server enable traps entity entity_power_status_change
no snmp-server enable traps entity entity_module_inserted
no snmp-server enable traps entity entity_module_removed
no snmp-server enable traps entity entity_unrecognised_module
no snmp-server enable traps entity entity_fan_status_change
no snmp-server enable traps entity entity_power_out_change
no snmp-server enable traps link linkDown
no snmp-server enable traps link linkUp
no snmp-server enable traps link IETF-extended-linkDown
no snmp-server enable traps link IETF-extended-linkUp
no snmp-server enable traps link cisco-extended-linkDown
no snmp-server enable traps link cisco-extended-linkUp
snmp-server enable traps callhome event-notify
snmp-server enable traps callhome smtp-send-fail
snmp-server enable traps cfs state-change-notif
snmp-server enable traps cfs merge-failure
no snmp-server enable traps rf redundancy_framework
```

```
snmp-server enable traps aaa server-state-change
no snmp-server enable traps license notify-license-expiry
no snmp-server enable traps license notify-no-license-for-feature
no snmp-server enable traps license notify-licensefile-missing
no snmp-server enable traps license notify-license-expiry-warning
snmp-server enable traps hsrp state-change
no snmp-server enable traps upgrade UpgradeOpNotifyOnCompletion
no snmp-server enable traps upgrade UpgradeJobStatusNotify
snmp-server enable traps feature-control FeatureOpStatusChange
snmp-server enable traps link cisco-xcvr-mon-status-chg
snmp-server enable traps vtp notifs
snmp-server enable traps vtp vlancreate
snmp-server enable traps vtp vlandelete
snmp-server enable traps bridge newroot
snmp-server enable traps bridge topologychange
snmp-server enable traps stpx inconsistency
snmp-server enable traps stpx root-inconsistency
snmp-server enable traps stpx loop-inconsistency
aaa authentication login default group CiscoACS
aaa authorization ssh-certificate default group CiscoACS
aaa accounting default group CiscoACS
aaa authentication login error-enable

vrf context VPC
vrf context servers1
  ip route 0.0.0.0/0 192.168.162.1
  ip route 192.168.41.0/24 192.168.42.135
  ip pim ssm range 232.0.0.0/8
vrf context servers2
  ip pim ssm range 232.0.0.0/8
vrf context management
vlan 1
vlan 36
  name DeviceMgmtHigh
vlan 37
  name DeviceMgmtLow
vlan 38
  name UIM-OS-INSTALL
vlan 40-41
vlan 42
  name CoreManagement
vlan 43
  name WirelessSystems
vlan 44
  name PhysicalSec
vlan 45
  name VOICE
vlan 52
  name POS
vlan 151-152,154,161-162,164,180-181
spanning-tree domain 777
spanning-tree vlan 1 priority 4096
ip prefix-list VLAN41 seq 5 permit 192.168.41.0/24
route-map VLAN41 permit 20
  match ip address prefix-list VLAN41
vpc domain 99
  peer-switch
  peer-keepalive destination 192.168.10.66 source 192.168.10.65 vrf VPC
  peer-gateway


interface Vlan1
  no shutdown
  no ip redirects
```

```
interface Vlan36
  no shutdown
  description DeviceMgmtHigh
  vrf member servers1
  no ip redirects
  ip address 192.168.36.3/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 2
    authentication text c1sc0
    preempt delay minimum 180
    priority 110 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.36.1

interface Vlan37
  no shutdown
  description DeviceMgmtLow
  vrf member servers1
  no ip redirects
  ip address 192.168.37.3/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 2
    authentication text c1sc0
    preempt delay minimum 180
    priority 110 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.37.1

interface Vlan38
  no shutdown
  description UIM OS Install only
  vrf member servers1
  no ip redirects
  ip address 192.168.38.201/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3

interface Vlan40
  no shutdown
  vrf member servers1
  no ip redirects
  ip address 192.168.40.3/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 2
    authentication text c1sc0
    preempt delay minimum 180
    priority 120 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.40.1

interface Vlan41
  shutdown
```

```
  description SHUTDOWN - NOW ROUTE VIA HyTrust
  vrf member servers1
  no ip redirects
  ip address 192.168.41.3/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 2
    authentication text c1sc0
    preempt delay minimum 180
    priority 120 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.41.1

interface Vlan42
  no shutdown
  vrf member servers1
  no ip redirects
  ip address 192.168.42.3/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 2
    authentication text c1sc0
    preempt delay minimum 180
    priority 120 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.42.1

interface Vlan43
  no shutdown
  description Wireless Systems
  vrf member servers1
  no ip redirects
  ip address 192.168.43.3/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 2
    authentication text c1sc0
    preempt delay minimum 180
    priority 110 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.43.1

interface Vlan44
  no shutdown
  description Wireless Systems
  vrf member servers1
  no ip redirects
  ip address 192.168.44.3/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 2
    authentication text c1sc0
    preempt delay minimum 180
    priority 110 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.44.1
```

```
interface Vlan45
  no shutdown
  description VOICE
  vrf member servers1
  no ip redirects
  ip address 192.168.45.3/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 2
    authentication text c1sc0
    preempt delay minimum 180
    priority 110 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.45.1

interface Vlan52
  no shutdown
  description POS
  vrf member servers1
  no ip redirects
  ip address 192.168.52.3/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 2
    authentication text c1sc0
    preempt delay minimum 180
    priority 110 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.52.1

interface Vlan154
  no shutdown
  vrf member servers2
  no ip redirects
  ip address 192.168.152.5/24
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 3 <removed>
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 2
    authentication text c1sc0
    preempt delay minimum 180
    priority 110 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.152.7

interface Vlan164
  no shutdown
  vrf member servers1
  no ip redirects
  ip address 192.168.162.5/24
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 3 <removed>
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 2
    authentication text c1sc0
```

```
    preempt delay minimum 180
    priority 120 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.162.7

interface Vlan180
  no shutdown
  vrf member servers1
  no ip redirects
  ip address 192.168.180.3/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 1
    authentication text c1sc0
    preempt delay minimum 180
    priority 120 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.180.1

interface Vlan181
  no shutdown
  vrf member servers2
  no ip redirects
  ip address 192.168.181.3/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 1
    authentication text c1sc0
    preempt delay minimum 180
    priority 110 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.181.1

interface port-channel1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-42,44
  vpc 1

interface port-channel2
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-42,44
  vpc 2

interface port-channel3
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  vpc 3

interface port-channel4
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  vpc 4

interface port-channel11
  switchport
  switchport mode trunk
```

```
  switchport trunk allowed vlan 38,41,45-46
  spanning-tree port type edge trunk
  vpc 11

interface port-channel12
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41,45-46
  spanning-tree port type edge trunk
  vpc 12

interface port-channel99
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 36-52
  spanning-tree port type network
  spanning-tree guard loop
  vpc peer-link

interface Ethernet1/2
  description F-UCS-1_E2/1 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41,45-46
  channel-group 11 mode active
  no shutdown

interface Ethernet1/4
  description F-UCS-1_E2/2 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41,45-46
  channel-group 11 mode active
  no shutdown

interface Ethernet1/6
  description F-UCS-2_E2/1 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41,45-46
  channel-group 12 mode active
  no shutdown

interface Ethernet1/8
  description F-UCS-2_E2/2 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41,45-46
  channel-group 12 mode active
  no shutdown

interface Ethernet1/9
  description SACCESS-3 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  channel-group 3 mode active
  no shutdown

interface Ethernet1/10
  description SACCESS-3 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
```

```
  channel-group 3 mode active
  no shutdown

interface Ethernet1/11
  description SACCESS-4 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  channel-group 4 mode active
  no shutdown

interface Ethernet1/12
  description SACCESS-4 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  channel-group 4 mode active
  no shutdown

interface Ethernet1/13
  description SACCESS-1 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-42,44
  channel-group 1 mode active
  no shutdown

interface Ethernet1/14
  description SACCESS-2 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-42,44
  channel-group 2 mode active
  no shutdown

interface Ethernet1/15
  description to RSERV-1 T2/1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 162
  spanning-tree port type normal
  no shutdown

interface Ethernet1/16
  description to RSERV-1 T2/2
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 152
  spanning-tree port type normal
  no shutdown

interface Ethernet1/17
  description to RSERV-1 T2/5
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 41-44,164
  spanning-tree port type normal
  no shutdown

interface Ethernet1/18
  description to RSERV-1 T2/6
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 154
```

```
  spanning-tree port type normal
  no shutdown

interface Ethernet1/19
  description to DC-ASA-1 vc1 T5/1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 162
  spanning-tree port type normal
  no shutdown

interface Ethernet1/20
  description to DC-ASA-1 vc2 T7/1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 152
  spanning-tree port type normal
  no shutdown

interface Ethernet1/21
  description RAGG-2 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 36-52
  udld aggressive
  channel-group 99 mode active
  no shutdown

interface Ethernet1/22
  description RAGG-2 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 36-52
  udld aggressive
  channel-group 99 mode active
  no shutdown

interface Ethernet1/23
  description RAGG-2 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 36-52
  udld aggressive
  channel-group 99 mode active
  no shutdown

interface Ethernet1/24
  description RAGG-2 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 36-52
  udld aggressive
  channel-group 99 mode active
  no shutdown

interface Ethernet2/13
  description SACCESS-5
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 36-52
  no shutdown

interface Ethernet2/14
  description linkstate for vpc
```

```
  no switchport
  vrf member VPC
  ip address 192.168.10.65/30
  no shutdown

interface Ethernet2/15
  no switchport

interface Ethernet2/16
  no switchport

interface Ethernet2/17
  no switchport

interface Ethernet2/18
  no switchport

interface Ethernet2/19
  no switchport

interface Ethernet2/20
  no switchport

interface Ethernet2/21
  no switchport

interface Ethernet2/22
  no switchport

interface Ethernet2/23
  no switchport

interface Ethernet2/24
  no switchport

interface Ethernet2/25
  no switchport

interface Ethernet2/26
  no switchport

interface Ethernet2/27
  no switchport

interface Ethernet2/28
  no switchport

interface Ethernet2/29
  no switchport

interface Ethernet2/30
  no switchport

interface Ethernet2/31
  no switchport

interface Ethernet2/32
  no switchport

interface Ethernet2/33
  no switchport

interface Ethernet2/34
  no switchport
```

```
interface Ethernet2/35
  no switchport

interface Ethernet2/36
  no switchport

interface Ethernet2/37
  no switchport

interface Ethernet2/38
  no switchport

interface Ethernet2/39
  no switchport

interface Ethernet2/40
  no switchport

interface Ethernet2/41
  no switchport

interface Ethernet2/42
  no switchport

interface Ethernet2/43
  no switchport

interface Ethernet2/44
  no switchport

interface Ethernet2/45
  no switchport

interface Ethernet2/46
  no switchport

interface Ethernet2/47
  no switchport

interface Ethernet2/48
  no switchport

interface loopback0
  vrf member servers1
  ip address 192.168.1.31/32
  ip router ospf 5 area 0.0.0.81
logging server 192.168.42.124 6 use-vrf servers1
logging source-interface loopback 0
  logout-warning 20
line console
  exec-timeout 15
line vty
  exec-timeout 15
  access-class 23 in
router ospf 5
  vrf servers1
    router-id 4.4.4.1
    area 0.0.0.81 nssa
    redistribute static route-map VLAN41
    area 0.0.0.81 range 192.168.0.0/16
    area 0.0.0.81 range 192.168.162.0/24
    area 0.0.0.81 authentication message-digest
    timers throttle spf 10 100 5000
```

```
  vrf servers2
    router-id 5.5.5.1
    area 0.0.0.81 nssa
    area 0.0.0.81 range 192.168.0.0/16
    area 0.0.0.81 range 192.168.152.0/24
    area 0.0.0.81 authentication message-digest
    timers throttle spf 10 100 5000
ip pim ssm range 232.0.0.0/8
```

RAGG-2-RUNNING

```
version 5.1(2)
hostname RAGG-2
vdc RAGG-2 id 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource monitor-session minimum 0 maximum 2
  limit-resource monitor-session-erspan-dst minimum 0 maximum 23
  limit-resource vrf minimum 2 maximum 1000
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 32 maximum 32
  limit-resource u6route-mem minimum 16 maximum 16
  limit-resource m4route-mem minimum 48 maximum 48
  limit-resource m6route-mem minimum 8 maximum 8
vdc vdc1 id 2
  allocate interface Ethernet1/1,Ethernet1/3,Ethernet1/5,Ethernet1/7,Ethernet1/25-32
  allocate interface Ethernet2/1-12
  boot-order 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource monitor-session minimum 0 maximum 2
  limit-resource monitor-session-erspan-dst minimum 0 maximum 23
  limit-resource vrf minimum 2 maximum 1000
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 8 maximum 8
  limit-resource u6route-mem minimum 4 maximum 4
  limit-resource m4route-mem minimum 8 maximum 8
  limit-resource m6route-mem minimum 5 maximum 5
vdc vdc2 id 3
  allocate interface Ethernet1/2,Ethernet1/4,Ethernet1/6,Ethernet1/8-24
  allocate interface Ethernet2/13-48
  boot-order 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource monitor-session minimum 0 maximum 2
  limit-resource monitor-session-erspan-dst minimum 0 maximum 23
  limit-resource vrf minimum 2 maximum 1000
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 8 maximum 8
  limit-resource u6route-mem minimum 4 maximum 4
  limit-resource m4route-mem minimum 8 maximum 8
  limit-resource m6route-mem minimum 5 maximum 5

feature privilege
feature tacacs+

username bart password 5 <removed> role network-admin
username bmcgloth password 5 <removed> role network-admin
enable secret 5 <removed>

banner motd @
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
```

```
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
@

ssh login-attempts 6

ip domain-lookup
ip domain-name cisco-irn.com
ip host RAGG-2 192.168.42.37
tacacs-server key 7 "<removed>"
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
    use-vrf management
ip access-list 23
  statistics per-entry
  10 permit ip 127.0.0.1/32 192.168.42.37/32
  20 permit ip 192.168.41.101/32 192.168.42.37/32
  30 permit ip 192.168.41.102/32 192.168.42.37/32
  40 permit ip 192.168.42.111/32 192.168.42.37/32
  50 permit ip 192.168.42.122/32 192.168.42.37/32
  60 permit ip 192.168.42.131/32 192.168.42.37/32
  70 permit ip 192.168.42.133/32 192.168.42.37/32
  80 permit ip 192.168.42.138/32 192.168.42.37/32
  90 permit ip 10.19.151.99/32 192.168.42.37/32
  100 deny ip any any
ip access-list 88
  statistics per-entry
  10 permit ip 192.168.42.122/32 192.168.42.37/32
  20 deny ip any any
ip access-list copp-system-acl-bgp
  10 permit tcp any gt 1024 any eq bgp
  20 permit tcp any eq bgp any gt 1024
ipv6 access-list copp-system-acl-bgp6
  10 permit tcp any gt 1024 any eq bgp
  20 permit tcp any eq bgp any gt 1024
ip access-list copp-system-acl-eigrp
  10 permit eigrp any any
ip access-list copp-system-acl-ftp
  10 permit tcp any any eq ftp-data
  20 permit tcp any any eq ftp
  30 permit tcp any eq ftp-data any
  40 permit tcp any eq ftp any
ip access-list copp-system-acl-glbp
  10 permit udp any eq 3222 224.0.0.0/24 eq 3222
ip access-list copp-system-acl-hsrp
  10 permit udp any 224.0.0.0/24 eq 1985
ip access-list copp-system-acl-icmp
  10 permit icmp any any echo
  20 permit icmp any any echo-reply
ipv6 access-list copp-system-acl-icmp6
  10 permit icmp any any echo-request
  20 permit icmp any any echo-reply
ipv6 access-list copp-system-acl-icmp6-msgs
  10 permit icmp any any router-advertisement
```

```
  20 permit icmp any any router-solicitation
  30 permit icmp any any nd-na
  40 permit icmp any any nd-ns
  50 permit icmp any any mld-query
  60 permit icmp any any mld-report
  70 permit icmp any any mld-reduction
ip access-list copp-system-acl-igmp
  10 permit igmp any 224.0.0.0/3
ip access-list copp-system-acl-msdp
  10 permit tcp any gt 1024 any eq 639
  20 permit tcp any eq 639 any gt 1024
ip access-list copp-system-acl-ntp
  10 permit udp any any eq ntp
  20 permit udp any eq ntp any
ipv6 access-list copp-system-acl-ntp6
  10 permit udp any any eq ntp
  20 permit udp any eq ntp any
ip access-list copp-system-acl-ospf
  10 permit ospf any any
ipv6 access-list copp-system-acl-ospf6
  10 permit 89 any any
ip access-list copp-system-acl-pim
  10 permit pim any 224.0.0.0/24
  20 permit udp any any eq pim-auto-rp
ip access-list copp-system-acl-pim-reg
  10 permit pim any any
ipv6 access-list copp-system-acl-pim6
  10 permit 103 any ff02::d/128
  20 permit udp any any eq pim-auto-rp
ip access-list copp-system-acl-radius
  10 permit udp any any eq 1812
  20 permit udp any any eq 1813
  30 permit udp any any eq 1645
  40 permit udp any any eq 1646
  50 permit udp any eq 1812 any
  60 permit udp any eq 1813 any
  70 permit udp any eq 1645 any
  80 permit udp any eq 1646 any
ipv6 access-list copp-system-acl-radius6
  10 permit udp any any eq 1812
  20 permit udp any any eq 1813
  30 permit udp any any eq 1645
  40 permit udp any any eq 1646
  50 permit udp any eq 1812 any
  60 permit udp any eq 1813 any
  70 permit udp any eq 1645 any
  80 permit udp any eq 1646 any
ip access-list copp-system-acl-rip
  10 permit udp any 224.0.0.0/24 eq rip
ip access-list copp-system-acl-sftp
  10 permit tcp any any eq 115
  20 permit tcp any eq 115 any
ip access-list copp-system-acl-snmp
  10 permit udp any any eq snmp
  20 permit udp any any eq snmptrap
ip access-list copp-system-acl-ssh
  10 permit tcp any any eq 22
  20 permit tcp any eq 22 any
ipv6 access-list copp-system-acl-ssh6
  10 permit tcp any any eq 22
  20 permit tcp any eq 22 any
ip access-list copp-system-acl-tacacs
  10 permit tcp any any eq tacacs
  20 permit tcp any eq tacacs any
```

```
ipv6 access-list copp-system-acl-tacacs6
  10 permit tcp any any eq tacacs
  20 permit tcp any eq tacacs any
ip access-list copp-system-acl-telnet
  10 permit tcp any any eq telnet
  20 permit tcp any any eq 107
  30 permit tcp any eq telnet any
  40 permit tcp any eq 107 any
ipv6 access-list copp-system-acl-telnet6
  10 permit tcp any any eq telnet
  20 permit tcp any any eq 107
  30 permit tcp any eq telnet any
  40 permit tcp any eq 107 any
ip access-list copp-system-acl-tftp
  10 permit udp any any eq tftp
  20 permit udp any any eq 1758
  30 permit udp any eq tftp any
  40 permit udp any eq 1758 any
ipv6 access-list copp-system-acl-tftp6
  10 permit udp any any eq tftp
  20 permit udp any any eq 1758
  30 permit udp any eq tftp any
  40 permit udp any eq 1758 any
ip access-list copp-system-acl-traceroute
  10 permit icmp any any ttl-exceeded
  20 permit icmp any any port-unreachable
ip access-list copp-system-acl-undesirable
  10 permit udp any any eq 1434
ip access-list copp-system-acl-vpc
  10 permit udp any any eq 3200
ip access-list copp-system-acl-vrrp
  10 permit 112 any 224.0.0.0/24
class-map type control-plane match-any copp-system-class-critical
  match access-group name copp-system-acl-bgp
  match access-group name copp-system-acl-bgp6
  match access-group name copp-system-acl-eigrp
  match access-group name copp-system-acl-igmp
  match access-group name copp-system-acl-msdp
  match access-group name copp-system-acl-ospf
  match access-group name copp-system-acl-ospf6
  match access-group name copp-system-acl-pim
  match access-group name copp-system-acl-pim6
  match access-group name copp-system-acl-rip
  match access-group name copp-system-acl-vpc
class-map type control-plane match-any copp-system-class-exception
  match exception ip option
  match exception ip icmp unreachable
  match exception ipv6 option
  match exception ipv6 icmp unreachable
class-map type control-plane match-any copp-system-class-important
  match access-group name copp-system-acl-glbp
  match access-group name copp-system-acl-hsrp
  match access-group name copp-system-acl-vrrp
  match access-group name copp-system-acl-icmp6-msgs
  match access-group name copp-system-acl-pim-reg
class-map type control-plane match-any copp-system-class-management
  match access-group name copp-system-acl-ftp
  match access-group name copp-system-acl-ntp
  match access-group name copp-system-acl-ntp6
  match access-group name copp-system-acl-radius
  match access-group name copp-system-acl-sftp
  match access-group name copp-system-acl-snmp
  match access-group name copp-system-acl-ssh
  match access-group name copp-system-acl-ssh6
```

```
  match access-group name copp-system-acl-tacacs
  match access-group name copp-system-acl-telnet
  match access-group name copp-system-acl-tftp
  match access-group name copp-system-acl-tftp6
  match access-group name copp-system-acl-radius6
  match access-group name copp-system-acl-tacacs6
  match access-group name copp-system-acl-telnet6
class-map type control-plane match-any copp-system-class-monitoring
  match access-group name copp-system-acl-icmp
  match access-group name copp-system-acl-icmp6
  match access-group name copp-system-acl-traceroute
class-map type control-plane match-any copp-system-class-normal
  match protocol arp
class-map type control-plane match-any copp-system-class-redirect
  match redirect dhcp-snoop
  match redirect arp-inspect
class-map type control-plane match-any copp-system-class-undesirable
  match access-group name copp-system-acl-undesirable
policy-map type control-plane copp-system-policy
  class copp-system-class-critical
    police cir 39600 kbps bc 250 ms conform transmit violate drop
  class copp-system-class-important
    police cir 1060 kbps bc 1000 ms conform transmit violate drop
  class copp-system-class-management
    police cir 10000 kbps bc 250 ms conform transmit violate drop
  class copp-system-class-normal
    police cir 680 kbps bc 250 ms conform transmit violate drop
  class copp-system-class-redirect
    police cir 280 kbps bc 250 ms conform transmit violate drop
  class copp-system-class-monitoring
    police cir 130 kbps bc 1000 ms conform transmit violate drop
  class copp-system-class-exception
    police cir 360 kbps bc 250 ms conform transmit violate drop
  class copp-system-class-undesirable
    police cir 32 kbps bc 250 ms conform drop violate drop
  class class-default
    police cir 100 kbps bc 250 ms conform transmit violate drop
control-plane
  service-policy input copp-system-policy
snmp-server user bmcgloth network-admin auth md5 <removed> priv <removed> localizedkey
ntp server 192.168.62.161 use-vrf management
ntp server 192.168.62.162 use-vrf management
aaa authentication login default group CiscoACS
aaa authentication login console group CiscoACS
aaa authorization ssh-certificate default group CiscoACS
aaa accounting default group CiscoACS
aaa authentication login error-enable

vrf context management
  ip route 0.0.0.0/0 192.168.42.1
vlan 1

interface mgmt0
  ip address 192.168.42.37/24
clock timezone PST -8 0
clock summer-time PST 1 Sun April 02:00 5 Sun Oct 02:00 60
  logout-warning 20
line console
  exec-timeout 15
line vty
  exec-timeout 15
  access-class 23 in
boot kickstart bootflash:/n7000-s1-kickstart.5.1.2.bin sup-1
boot system bootflash:/n7000-s1-dk9.5.1.2.bin sup-1
```

```
boot kickstart bootflash:/n7000-s1-kickstart.5.1.2.bin sup-2
boot system bootflash:/n7000-s1-dk9.5.1.2.bin sup-2
logging server 192.168.42.124 6 use-vrf management
```

RAGG-2-VDC1-RUNNING

```
version 5.1(2)
hostname vdc1

feature privilege
feature tacacs+
cfs eth distribute
feature ospf
feature pim
feature udld
feature interface-vlan
feature hsrp
feature lacp
feature glbp
feature vpc

username bmcgloth password 5 <removed>   role vdc-admin
username bart password 5 <removed>   role vdc-admin
enable secret 5 <removed>

banner motd @
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                  **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
@

ssh login-attempts 6

ip domain-lookup
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
tacacs-server key 7 "<removed>"
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
    source-interface loopback0
ip access-list 23
  statistics per-entry
  10 permit ip 127.0.0.1/32 192.168.1.12/32
  20 permit ip 192.168.41.101/32 192.168.1.12/32
  30 permit ip 192.168.41.102/32 192.168.1.12/32
  40 permit ip 192.168.42.111/32 192.168.1.12/32
  50 permit ip 192.168.42.122/32 192.168.1.12/32
  60 permit ip 192.168.42.131/32 192.168.1.12/32
  70 permit ip 192.168.42.133/32 192.168.1.12/32
```

```
  80 permit ip 192.168.42.138/32 192.168.1.12/32
  90 permit ip 10.19.151.99/32 192.168.1.12/32
  100 deny ip any any
ip access-list 88
  statistics per-entry
  10 permit ip 192.168.42.122/32 192.168.1.12/32
  20 deny ip any any
snmp-server user bmcgloth vdc-admin auth md5 <removed> priv <removed> localizedkey
aaa authentication login default group CiscoACS
aaa authorization ssh-certificate default group CiscoACS
aaa accounting default group CiscoACS
aaa authentication login error-enable

vrf context management
vlan 1,3,151,161

interface Vlan1

interface Vlan3
  no shutdown
  ip address 192.168.10.62/30
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 3 <removed>
  ip ospf dead-interval 3
  ip ospf hello-interval 1
  ip router ospf 5 area 0.0.0.0

interface Vlan151
  no shutdown
  ip address 192.168.152.4/24
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 3 <removed>
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 1
    authentication text c1sc0
    preempt delay minimum 180
    priority 10 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.152.1

interface Vlan161
  no shutdown
  ip address 192.168.162.4/24
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 3 <removed>
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 1
    authentication text c1sc0
    preempt delay minimum 180
    priority 10 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.162.1

interface port-channel99
  switchport
  switchport mode trunk
  spanning-tree port type network

interface Ethernet1/1
  description 10Gig LINK to RCORE-1 T2/2
```

```
  no switchport
  logging event port link-status
  no ip redirects
  ip address 192.168.10.18/30
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 3 <removed>
  ip ospf dead-interval 6
  ip ospf hello-interval 2
  ip ospf network point-to-point
  ip router ospf 5 area 0.0.0.0
  ip pim sparse-mode
  ip igmp version 3
  no shutdown

interface Ethernet1/3
  description 10Gig LINK to RCORE-2 T2/2
  no switchport
  logging event port link-status
  no ip redirects
  ip address 192.168.10.26/30
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 3 <removed>
  ip ospf dead-interval 6
  ip ospf hello-interval 2
  ip ospf network point-to-point
  ip router ospf 5 area 0.0.0.0
  ip pim sparse-mode
  ip igmp version 3
  no shutdown

interface Ethernet1/5
  description to DC-ASA-2 vc1 T0/6
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 161
  spanning-tree port type normal
  no shutdown

interface Ethernet1/7
  description to DC-ASA-2 vc2 T0/8
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 151
  spanning-tree port type normal
  no shutdown

interface Ethernet1/25
  no switchport

interface Ethernet1/26
  no switchport

interface Ethernet1/27
  no switchport

interface Ethernet1/28
  no switchport

interface Ethernet1/29
  description RAGG-1 vPC Channel link
  switchport
  switchport mode trunk
  channel-group 99 mode active
  no shutdown
```

```
interface Ethernet1/30
  description RAGG-1 vPC Channel link
  switchport
  switchport mode trunk
  channel-group 99 mode active
  no shutdown

interface Ethernet1/31
  description RAGG-1 vPC Channel link
  switchport
  switchport mode trunk
  channel-group 99 mode active
  no shutdown

interface Ethernet1/32
  description RAGG-1 vPC Channel link
  switchport
  switchport mode trunk
  channel-group 99 mode active
  no shutdown

interface Ethernet2/1
  no switchport

interface Ethernet2/2
  no switchport

interface Ethernet2/3
  no switchport

interface Ethernet2/4
  no switchport

interface Ethernet2/5
  no switchport

interface Ethernet2/6
  no switchport

interface Ethernet2/7
  no switchport

interface Ethernet2/8
  no switchport

interface Ethernet2/9
  no switchport

interface Ethernet2/10
  no switchport

interface Ethernet2/11
  no switchport

interface Ethernet2/12
  no switchport

interface loopback0
  ip address 192.168.1.12/32
  ip router ospf 5 area 0.0.0.0
logging server 192.168.42.124 6
logging source-interface loopback 0
  logout-warning 20
```

```
line console
  exec-timeout 15
line vty
  exec-timeout 15
  access-class 23 in
router ospf 5
  router-id 192.168.1.12
  area 0.0.0.81 nssa
  area 0.0.0.0 range 192.168.1.12/32
  area 0.0.0.0 range 192.168.10.12/30
  area 0.0.0.0 range 192.168.10.20/30
  area 0.0.0.0 range 192.168.10.60/30
  area 0.0.0.81 range 192.168.152.0/24
  area 0.0.0.81 range 192.168.162.0/24
  area 0.0.0.0 authentication message-digest
  area 0.0.0.81 authentication message-digest
  timers throttle spf 10 100 5000
  auto-cost reference-bandwidth 10000
ip pim ssm range 232.0.0.0/8
```

RAGG-2-VDC2-RUNNING

```
version 5.1(2)
hostname vdc2

feature privilege
feature tacacs+
cfs eth distribute
feature ospf
feature pim
feature udld
feature interface-vlan
feature hsrp
feature lacp
feature dhcp
feature vpc

username bart password 5 <removed>   role vdc-admin
username bmcgloth password 5 <removed>   role vdc-admin
enable secret 5 <removed>

banner motd @
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                  **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
@

ssh login-attempts 6

ip domain-lookup
```

```
ip domain-name cisco-irn.com
tacacs-server key 7 "<removed>"
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
    use-vrf servers1
    source-interface loopback0
ip access-list 23
  statistics per-entry
  10 permit ip 127.0.0.1/32 192.168.1.32/32
  20 permit ip 192.168.41.101/32 192.168.1.32/32
  30 permit ip 192.168.41.102/32 192.168.1.32/32
  40 permit ip 192.168.42.111/32 192.168.1.32/32
  50 permit ip 192.168.42.122/32 192.168.1.32/32
  60 permit ip 192.168.42.131/32 192.168.1.32/32
  70 permit ip 192.168.42.133/32 192.168.1.32/32
  80 permit ip 192.168.42.138/32 192.168.1.32/32
  90 permit ip 10.19.151.99/32 192.168.1.32/32
  100 deny ip any any
ip access-list 88
  statistics per-entry
  10 permit ip 192.168.42.122/32 192.168.1.32/32
  20 deny ip any any
snmp-server user bmcgloth vdc-admin auth md5 <removed> priv <removed> localizedkey
aaa authentication login default group CiscoACS
aaa authorization ssh-certificate default group CiscoACS
aaa accounting default group CiscoACS
aaa authentication login error-enable

vrf context VPC
vrf context servers1
  ip route 0.0.0.0/0 192.168.36.3
  ip pim ssm range 232.0.0.0/8
vrf context servers2
  ip pim ssm range 232.0.0.0/8
vrf context management
vlan 1
vlan 36
  name DeviceMgmtHigh
vlan 37
  name DeviceMgmtLow
vlan 38
  name UIM-OS-INSTALL
vlan 40-41
vlan 42
  name CoreManagement
vlan 43
  name WirelessSystems
vlan 44
  name PhysicalSec
vlan 45
  name VOICE
vlan 52
  name POS
vlan 151-152,154,161-162,164,180-181
spanning-tree domain 777
ip prefix-list VLAN41 seq 5 permit 192.168.41.0/24
route-map VLAN41 permit 20
  match ip address prefix-list VLAN41
service dhcp
ip dhcp relay
vpc domain 99
  peer-keepalive destination 192.168.10.65 source 192.168.10.66 vrf VPC
```

```
interface Vlan1
  no ip redirects
  no shutdown

interface Vlan36
  vrf member servers1
  no ip redirects
  ip address 192.168.36.4/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 2
    authentication text c1sc0
    preempt delay minimum 180
    priority 105 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.36.1
  no shutdown
  description DeviceMgmtHigh

interface Vlan37
  vrf member servers1
  no ip redirects
  ip address 192.168.37.4/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 2
    authentication text c1sc0
    preempt delay minimum 180
    priority 105 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.37.1
  no shutdown
  description DeviceMgmtLow

interface Vlan38
  vrf member servers1
  no ip redirects
  ip address 192.168.38.202/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  no shutdown
  description UIM OS Install only

interface Vlan40
  vrf member servers1
  no ip redirects
  ip address 192.168.40.4/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 2
    authentication text c1sc0
    preempt delay minimum 180
    priority 105 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.40.1
```

```
  no shutdown

interface Vlan41
  vrf member servers1
  ip address 192.168.41.4/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 2
    authentication text c1sc0
    preempt delay minimum 180
    priority 90 forwarding-threshold lower 1 upper 1
    timers  1  3
    ip 192.168.41.1
  shutdown
  description SHUTDOWN - NOW ROUTE VIA HyTrust

interface Vlan42
  vrf member servers1
  no ip redirects
  ip address 192.168.42.4/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 2
    authentication text c1sc0
    preempt delay minimum 180
    priority 105 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.42.1
  no shutdown

interface Vlan43
  vrf member servers1
  no ip redirects
  ip address 192.168.43.4/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 2
    authentication text c1sc0
    preempt delay minimum 180
    priority 105 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.43.1
  no shutdown
  description Wireless Systems

interface Vlan44
  vrf member servers1
  no ip redirects
  ip address 192.168.44.4/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 2
    authentication text c1sc0
    preempt delay minimum 180
    priority 105 forwarding-threshold lower 0 upper 0
    timers  1  3
```

```
    ip 192.168.44.1
  no shutdown
  description Wireless Systems

interface Vlan45
  vrf member servers1
  no ip redirects
  ip address 192.168.45.4/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 2
    authentication text c1sc0
    preempt delay minimum 180
    priority 105 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.45.1
  no shutdown
  description VOICE

interface Vlan52
  vrf member servers1
  no ip redirects
  ip address 192.168.52.4/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 2
    authentication text c1sc0
    preempt delay minimum 180
    priority 105 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.52.1
  no shutdown
  description POS

interface Vlan154
  vrf member servers2
  no ip redirects
  ip address 192.168.152.6/24
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 3 <removed>
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 2
    authentication text c1sc0
    preempt delay minimum 180
    priority 120 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.152.7
  no shutdown

interface Vlan164
  vrf member servers1
  no ip redirects
  ip address 192.168.162.6/24
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 3 <removed>
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
```

```
  hsrp 2
    authentication text c1sc0
    preempt delay minimum 180
    priority 110 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.162.7
  no shutdown

interface Vlan180
  vrf member servers1
  no ip redirects
  ip address 192.168.180.4/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 1
    authentication text c1sc0
    preempt delay minimum 180
    priority 110 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.180.1
  no shutdown

interface Vlan181
  vrf member servers2
  no ip redirects
  ip address 192.168.181.4/24
  ip ospf passive-interface
  ip router ospf 5 area 0.0.0.81
  ip pim sparse-mode
  ip igmp version 3
  hsrp 1
    authentication text c1sc0
    preempt delay minimum 180
    priority 120 forwarding-threshold lower 0 upper 0
    timers  1  3
    ip 192.168.181.1
  no shutdown

interface port-channel1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-42,44
  vpc 1

interface port-channel2
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-42,44
  vpc 2

interface port-channel3
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  vpc 3

interface port-channel4
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  vpc 4
```

```
interface port-channel11
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41,45-46
  spanning-tree port type edge trunk
  vpc 11

interface port-channel12
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41,45-46
  spanning-tree port type edge trunk
  vpc 12

interface port-channel99
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 36-52
  spanning-tree port type network
  spanning-tree guard loop
  vpc peer-link

interface Ethernet1/2
  description F-UCS-1_E2/1 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41,45-46
  channel-group 11 mode active
  no shutdown

interface Ethernet1/4
  description F-UCS-1_E2/2 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41,45-46
  spanning-tree port type normal
  channel-group 11 mode active
  no shutdown

interface Ethernet1/6
  description F-UCS-2_E2/1 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41,45-46
  channel-group 12 mode active
  no shutdown

interface Ethernet1/8
  description F-UCS-2_E2/2 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41,45-46
  channel-group 12 mode active
  no shutdown

interface Ethernet1/9
  description SACCESS-3 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  channel-group 3 mode active
  no shutdown

interface Ethernet1/10
```

```
  description SACCESS-3 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  channel-group 3 mode active
  no shutdown

interface Ethernet1/11
  description SACCESS-4 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  channel-group 4 mode active
  no shutdown

interface Ethernet1/12
  description SACCESS-4 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  channel-group 4 mode active
  no shutdown

interface Ethernet1/13
  description SACCESS-1 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-42,44
  channel-group 1 mode active
  no shutdown

interface Ethernet1/14
  description SACCESS-2 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 38,41-42,44
  channel-group 2 mode active
  no shutdown

interface Ethernet1/15
  no switchport

interface Ethernet1/16
  no switchport

interface Ethernet1/17
  description to RSERV-2 T2/6
  switchport
  switchport mode trunk
  spanning-tree port type normal
  no shutdown

interface Ethernet1/18
  description to RSERV-2 T2/5
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 42,164
  no shutdown

interface Ethernet1/19
  description to DC-ASA-2 vc1 T5/1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 152
```

```
  spanning-tree port type normal
  no shutdown

interface Ethernet1/20
  description to DC-ASA-2 vc2 T7/1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 152
  spanning-tree port type normal
  no shutdown

interface Ethernet1/21
  description RAGG-2 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 36-52
  udld aggressive
  channel-group 99 mode active
  no shutdown

interface Ethernet1/22
  description RAGG-2 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 36-52
  udld aggressive
  channel-group 99 mode active
  no shutdown

interface Ethernet1/23
  description RAGG-2 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 36-52
  udld aggressive
  channel-group 99 mode active
  no shutdown

interface Ethernet1/24
  description RAGG-2 vPC Channel link
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 36-52
  udld aggressive
  channel-group 99 mode active
  no shutdown

interface Ethernet2/13
  description SACCESS-5 vPC Channel link
  switchport
  switchport mode trunk

interface Ethernet2/14
  description linkstate for vpc
  no switchport
  vrf member VPC
  ip address 192.168.10.66/30
  no shutdown

interface Ethernet2/15
  no switchport

interface Ethernet2/16
  no switchport
```

```
interface Ethernet2/17
  no switchport

interface Ethernet2/18
  no switchport

interface Ethernet2/19
  no switchport

interface Ethernet2/20
  no switchport

interface Ethernet2/21
  no switchport

interface Ethernet2/22
  no switchport

interface Ethernet2/23
  no switchport

interface Ethernet2/24
  no switchport

interface Ethernet2/25
  no switchport

interface Ethernet2/26
  no switchport

interface Ethernet2/27
  no switchport

interface Ethernet2/28
  no switchport

interface Ethernet2/29
  no switchport

interface Ethernet2/30
  no switchport

interface Ethernet2/31
  no switchport

interface Ethernet2/32
  no switchport

interface Ethernet2/33
  no switchport

interface Ethernet2/34
  no switchport

interface Ethernet2/35
  no switchport

interface Ethernet2/36
  no switchport

interface Ethernet2/37
  no switchport
```

```
interface Ethernet2/38
  no switchport

interface Ethernet2/39
  no switchport

interface Ethernet2/40
  no switchport

interface Ethernet2/41
  no switchport

interface Ethernet2/42
  no switchport

interface Ethernet2/43
  no switchport

interface Ethernet2/44
  no switchport

interface Ethernet2/45
  no switchport

interface Ethernet2/46
  no switchport

interface Ethernet2/47
  no switchport

interface Ethernet2/48
  no switchport

interface loopback0
  vrf member servers1
  ip address 192.168.1.32/32
  ip router ospf 5 area 0.0.0.81
logging server 192.168.42.124 6 use-vrf servers1
logging source-interface loopback 0
  logout-warning 20
line console
  exec-timeout 15
line vty
  exec-timeout 15
  access-class 23 in
router ospf 5
  vrf servers1
    router-id 4.4.4.2
    area 0.0.0.81 nssa
    area 0.0.0.81 range 192.168.0.0/16
    area 0.0.0.81 range 192.168.162.0/24
    area 0.0.0.81 authentication message-digest
    timers throttle spf 10 100 5000
  vrf servers2
    router-id 5.5.5.2
    area 0.0.0.81 nssa
    area 0.0.0.81 range 192.168.0.0/16
    area 0.0.0.81 range 192.168.152.0/24
    area 0.0.0.81 authentication message-digest
    timers throttle spf 10 100 5000
ip pim ssm range 232.0.0.0/8
```

N1KV-1-RUNNING

```
version 4.2(1)SV1(4)
no feature telnet
feature tacacs+

username bart password 5 <removed>   role network-admin
username bmcgloth password 5 <removed>   role network-admin

banner motd #
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
#

ssh key rsa 2048
ip domain-lookup
ip domain-lookup
tacacs-server key 7 "<removed>"
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
    use-vrf management
    source-interface mgmt0
aaa group server tacacs+ tacacs
hostname N1kv-1
ip access-list 23
  10 permit ip 192.168.42.0/24 any
  20 permit ip any any
  30 deny ip any any
ip access-list 88
  10 permit ip 192.168.42.0/24 any
  20 permit ip any any
  30 deny ip any any
vem 3
  host vmware id 414e3537-3441-3255-5838-34353034544b
vem 4
  host vmware id 414e3537-3441-3255-5838-34353034544d
vem 5
  host vmware id 414e3537-3441-3255-5838-333930345046
vem 6
  host vmware id 414e3537-3441-3255-5838-34353034544c
vem 7
  host vmware id 414e3537-3441-3255-5838-333930344e59
vem 8
  host vmware id 414e3537-3441-3255-5838-333830333330
vem 9
  host vmware id 414e3537-3441-3255-5838-333930345057
vem 10
  host vmware id 414e3537-3441-3255-5838-343530345630
vem 11
  host vmware id 414e3537-3441-3255-5838-343530345448
```

```
vem 12
  host vmware id 414e3537-3441-3255-5838-333930345048
snmp-server user bmcgloth network-admin auth md5 <removed> priv <removed> localizedkey
ntp server 192.168.62.161 use-vrf management
ntp server 192.168.62.162 use-vrf management
ntp source 192.168.41.61
aaa authentication login default group CiscoACS
aaa authentication login console group CiscoACS

vrf context management
  ip route 0.0.0.0/0 192.168.41.1
vlan 1
vlan 36
  name VLAN36
vlan 37
  name VLAN37
vlan 38
  name VLAN38
vlan 39
  name VLAN39
vlan 40
  name VLAN40
vlan 41
  name VLAN41
vlan 42
  name VLAN42
vlan 43
  name VLAN43
vlan 44
  name VLAN44
vlan 45
  name VLAN45
vlan 46
  name VLAN46
vlan 52
  name VLAN52
vlan 64
  name VLAN64
vlan 72
  name VLAN72
vlan 80
  name VLAN80
vlan 81
  name VLAN81
vlan 82
  name VLAN82
vlan 83
  name VLAN83
port-channel load-balance ethernet source-mac
port-profile default max-ports 32
port-profile type vethernet VLAN38
  vmware port-group
  switchport mode access
  switchport access vlan 38
  no shutdown
  state enabled
port-profile type vethernet VLAN36
  vmware port-group
  switchport mode access
  switchport access vlan 36
  no shutdown
  state enabled
port-profile type vethernet VLAN37
  vmware port-group
```

```
  switchport mode access
  switchport access vlan 37
  no shutdown
  state enabled
port-profile type vethernet VLAN39
  vmware port-group
  switchport mode access
  switchport access vlan 39
  no shutdown
  state enabled
port-profile type vethernet VLAN40
  vmware port-group
  switchport mode access
  switchport access vlan 40
  no shutdown
  state enabled
port-profile type vethernet VLAN41
  vmware port-group
  switchport mode access
  switchport access vlan 41
  no shutdown
  system vlan 41
  state enabled
port-profile type vethernet VLAN42
  vmware port-group
  switchport mode access
  switchport access vlan 42
  no shutdown
  state enabled
port-profile type vethernet VLAN43
  vmware port-group
  switchport mode access
  switchport access vlan 43
  no shutdown
  state enabled
port-profile type vethernet VLAN44
  vmware port-group
  switchport mode access
  switchport access vlan 44
  no shutdown
  state enabled
port-profile type vethernet VLAN45
  vmware port-group
  switchport mode access
  switchport access vlan 45
  no shutdown
  state enabled
port-profile type vethernet VLAN46
  vmware port-group
  switchport mode access
  switchport access vlan 46
  no shutdown
  state enabled
port-profile type vethernet VLAN52
  vmware port-group
  switchport mode access
  switchport access vlan 52
  no shutdown
  state enabled
port-profile type vethernet VLAN64
  vmware port-group
  switchport mode access
  switchport access vlan 64
  no shutdown
```

```
  state enabled
port-profile type vethernet VLAN72
  vmware port-group
  switchport mode access
  switchport access vlan 72
  no shutdown
  state enabled
port-profile type vethernet VLAN80
  vmware port-group
  switchport mode access
  switchport access vlan 80
  no shutdown
  state enabled
port-profile type vethernet VLAN81
  vmware port-group
  switchport mode access
  switchport access vlan 81
  no shutdown
  state enabled
port-profile type vethernet VLAN82
  vmware port-group
  switchport mode access
  switchport access vlan 82
  no shutdown
  state enabled
port-profile type vethernet VLAN83
  vmware port-group
  switchport mode access
  switchport access vlan 83
  no shutdown
  state enabled
port-profile type ethernet Unused_Or_Quarantine_Uplink
  vmware port-group
  shutdown
  description Port-group created for Nexus1000V internal usage. Do not use.
  state enabled
port-profile type vethernet Unused_Or_Quarantine_Veth
  vmware port-group
  shutdown
  description Port-group created for Nexus1000V internal usage. Do not use.
  state enabled
port-profile type ethernet sysuplink
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 36-83
  no shutdown
  system vlan 41
  state enabled
port-profile type vethernet VSG-DADA-HA
  vmware port-group
  switchport access vlan 41
  no shutdown
  state enabled
port-profile type vethernet Tenant-1
  vmware port-group
  org root/Tenant-1
  vn-service ip-address 192.168.52.11 vlan 52 security-profile SecurityProfile-1
  switchport mode access
  switchport access vlan 41
  no shutdown
  state enabled

vdc N1kv-1 id 1
  limit-resource vlan minimum 16 maximum 2049
```

```
  limit-resource monitor-session minimum 0 maximum 2
  limit-resource vrf minimum 16 maximum 8192
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 32 maximum 32
  limit-resource u6route-mem minimum 16 maximum 16
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8

interface mgmt0
  ip address 192.168.41.61/24

interface Vethernet3
  inherit port-profile VLAN42
  description RSA-Archer,Network Adapter 1
  vmware dvport 207 dvswitch uuid "f9 31 3b 50 f5 23 1c a3-34 b1 f1 a6 d6 24 6c c0"
  vmware vm mac 0050.56BB.001E

interface Vethernet5
  inherit port-profile VSG-DADA-HA
  description Nexus1000VSG,Network Adapter 3
  vmware dvport 1057 dvswitch uuid "f9 31 3b 50 f5 23 1c a3-34 b1 f1 a6 d6 24 6c c0"
  vmware vm mac 0050.56BB.0004

interface Vethernet6
  inherit port-profile VSG-DADA-HA
  description Nexus1000VSG,Network Adapter 1
  vmware dvport 1056 dvswitch uuid "f9 31 3b 50 f5 23 1c a3-34 b1 f1 a6 d6 24 6c c0"
  vmware vm mac 0050.56BB.0002

interface Vethernet7
  inherit port-profile VLAN52
  description POS Terminal,Network Adapter 1
  vmware dvport 352 dvswitch uuid "f9 31 3b 50 f5 23 1c a3-34 b1 f1 a6 d6 24 6c c0"
  vmware vm mac 0050.56BB.0005

interface control0
clock timezone PST -8 0
clock summer-time PST 1 Sun April 02:00 5 Sun Oct 02:00 60
line vty
  exec-timeout 15
line console
  exec-timeout 15
boot kickstart bootflash:/nexus-1000v-kickstart-mz.4.2.1.SV1.4.bin sup-1
boot system bootflash:/nexus-1000v-mz.4.2.1.SV1.4.bin sup-1
boot kickstart bootflash:/nexus-1000v-kickstart-mz.4.2.1.SV1.4.bin sup-2
boot system bootflash:/nexus-1000v-mz.4.2.1.SV1.4.bin sup-2
svs-domain
  domain id 2
  control vlan 41
  packet vlan 41
  svs mode L2
svs connection vc
  protocol vmware-vim
  remote ip address 192.168.41.102 port 80
  vmware dvs uuid "f9 31 3b 50 f5 23 1c a3-34 b1 f1 a6 d6 24 6c c0" datacenter-name
COMPLIANCE Lab
  connect
vnm-policy-agent
  registration-ip 192.168.41.65
  shared-secret **********
  policy-agent-image bootflash:/vnmc-vsmpa.1.0.1j.bin
  log-level
logging server 192.168.42.124 7 facility syslog
logging timestamp milliseconds
```

VSG-TENANT-1-RUNNING

```
version 4.2(1)VSG1(1)
no feature telnet
feature tacacs+

username bmcgloth password 5 <removed> role network-admin

banner motd #
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                  **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
#

ssh key rsa 2048
ip domain-lookup
ip domain-lookup
tacacs-server key 7 " <removed> "
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
    use-vrf management
    source-interface mgmt0
aaa group server tacacs+ tacacs
hostname VSG-Tenant-1
no snmp-server protocol enable
snmp-server user bmcgloth network-admin auth md5 <removed> priv <removed> localizedkey
ntp source 192.168.41.63
aaa authentication login default group CiscoACS
aaa authentication login console group CiscoACS

vrf context management
  ip domain-name cisco-irn.com
  ip name-server 192.168.42.130
  ip route 0.0.0.0/0 192.168.41.1
vlan 1
port-channel load-balance ethernet source-mac
port-profile default max-ports 32

vdc VSG-Tenant-1 id 1
  limit-resource vlan minimum 16 maximum 2049
  limit-resource monitor-session minimum 0 maximum 2
  limit-resource vrf minimum 16 maximum 8192
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 32 maximum 32
  limit-resource u6route-mem minimum 16 maximum 16
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8
```

```
interface mgmt0
  ip address 192.168.41.63/24

interface data0
  ip address 192.168.52.11/24
clock timezone PST -8 0
clock summer-time PST 1 Sun April 02:00 5 Sun Oct 02:00 60
line vty
  exec-timeout 15
line console
  exec-timeout 15
boot kickstart bootflash:/nexus-1000v-kickstart-mz.VSG1.1.bin sup-1
boot system bootflash:/nexus-1000v-mz.VSG1.1.bin sup-1
boot kickstart bootflash:/nexus-1000v-kickstart-mz.VSG1.1.bin sup-2
boot system bootflash:/nexus-1000v-mz.VSG1.1.bin sup-2
ip access-list match-local-traffic
  ha-pair id 41

security-profile SecurityProfile-1@root/Tenant-1
  policy PolicySet-A@root/Tenant-1
  custom-attribute vnsporg "root/tenant-1"

security-profile default@root
  policy default@root
  custom-attribute vnsporg "root"
rule default/default-rule@root
  action 10 drop
rule PolicyA/allow_ICMP@root/Tenant-1
  condition 10 dst.net.ip-address eq 192.168.1.1
  condition 11 net.protocol eq 1
  action 10 log
  action 11 permit
policy default@root
  rule default/default-rule@root order 2
policy PolicySet-A@root/Tenant-1
  rule PolicyA/allow_ICMP@root/Tenant-1 order 101
vnm-policy-agent
  registration-ip 192.168.41.65
  shared-secret **********
  policy-agent-image bootflash:/vnmc-vsgpa.1.0.1j.bin
  log-level
logging logfile messages 2
logging server 192.168.42.124 6 facility local0
logging monitor 2
```

RSERV-1

```
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
service counters max age 5
!
hostname RSERV-1
!
boot-start-marker
```

```
boot system flash sup-bootdisk:/s72033-adventerprisek9_wan-mz.122-33.SXJ.bin
boot-end-marker
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 50000
no logging rate-limit
enable secret 5 <removed>
!

username bart privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
aaa new-model
!
!
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
svclc module 4 vlan-group 162,163
svclc vlan-group 162  152,162
svclc vlan-group 163  153,163
intrusion-detection module 9 management-port access-vlan 42
intrusion-detection module 9 data-port 1 trunk allowed-vlan 153,154
intrusion-detection module 9 data-port 2 trunk allowed-vlan 163,164
ip wccp 61
ip wccp 62
!
!
!
no ip bootp server
ip multicast-routing
ip ssh version 2
ip scp server enable
no ip domain-lookup
ip domain-name cisco-irn.com
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
ipv6 mfib hardware-switching replication-mode ingress
vtp domain datacenter
vtp mode transparent
no mls acl tcam share-global
mls netflow interface
mls cef error action freeze
password encryption aes
!
crypto pki trustpoint TP-self-signed-1027
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1027
 revocation-check none
 rsakeypair TP-self-signed-1027
!
```

```
!
crypto pki certificate chain TP-self-signed-1027
 certificate self-signed 01
  <removed>
  quit
!
!
!
!
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
!
spanning-tree mode pvst
!
no power enable module 8
diagnostic bootup level minimal
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
redundancy
 main-cpu
  auto-sync running-config
 mode sso
!
!
vlan internal allocation policy descending
vlan dot1q tag native
vlan access-log ratelimit 2000
!
vlan 41
 name DeviceManagementHTA
!
vlan 42
 name DeviceManagement
!
vlan 43
 name WIRELESS-CONTROL
!
vlan 44
 name PhysicalSec
!
vlan 47
 name WAAS_Central_Manager
!
vlan 49
 name WAAS_DC
!
```

```
vlan 152
 name NorthSide_facing_ASA_Servers2
!
vlan 153
 name ACE_to_IDS_Servers2
!
vlan 154
 name SouthSide_facing_Servers2
!
vlan 162
 name NorthSide_facing_ASA_Servers1
!
vlan 163
 name ACE_to_IDS_Servers1
!
vlan 164
 name SouthSide_facing_Servers1
!
vlan 803
 name RSERV-1_to_RAGG-1-VDC-2
!
vlan 1000
!
!
!
!
!
interface Loopback0
 ip address 192.168.1.21 255.255.255.255
!
interface Loopback62
 ip address 192.168.62.161 255.255.255.255
!
interface GigabitEthernet1/1
 no ip address
 shutdown
!
interface GigabitEthernet1/2
 no ip address
 shutdown
!
interface GigabitEthernet1/3
 no ip address
 shutdown
!
interface GigabitEthernet1/4
 no ip address
 shutdown
!
interface GigabitEthernet1/5
 no ip address
 shutdown
!
interface GigabitEthernet1/6
 no ip address
 shutdown
!
interface GigabitEthernet1/7
 no ip address
 shutdown
!
interface GigabitEthernet1/8
 no ip address
 shutdown
```

```
!
interface GigabitEthernet1/9
 no ip address
 shutdown
!
interface GigabitEthernet1/10
 no ip address
 shutdown
!
interface GigabitEthernet1/11
 no ip address
 shutdown
!
interface GigabitEthernet1/12
 no ip address
 shutdown
!
interface GigabitEthernet1/13
 no ip address
 shutdown
!
interface GigabitEthernet1/14
 no ip address
 shutdown
!
interface GigabitEthernet1/15
 no ip address
 shutdown
!
interface GigabitEthernet1/16
 no ip address
 shutdown
!
interface TenGigabitEthernet2/1
 description to RAGG-1 vdc2 T1/15
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 162
 switchport mode trunk
!
interface TenGigabitEthernet2/2
 description to RAGG-1 vdc2 T1/16
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 152
 switchport mode trunk
!
interface TenGigabitEthernet2/3
 no ip address
 shutdown
!
interface TenGigabitEthernet2/4
 no ip address
 shutdown
!
interface TenGigabitEthernet2/5
 description to RAGG-1 vdc2 T1/17
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 41-44,164,803
 switchport mode trunk
!
interface TenGigabitEthernet2/6
 description to RAGG-1 vdc2 T1/18
```

```
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 154
 switchport mode trunk
!
interface TenGigabitEthernet2/7
 no ip address
 shutdown
!
interface TenGigabitEthernet2/8
 no ip address
 shutdown
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 no ip address
 shutdown
!
interface GigabitEthernet6/1
 no ip address
 shutdown
!
interface GigabitEthernet6/2
 no ip address
 shutdown
!
interface GigabitEthernet7/1
 no ip address
 shutdown
!
interface GigabitEthernet7/2
 no ip address
 shutdown
!
interface GigabitEthernet7/3
 no ip address
!
interface GigabitEthernet7/4
 no ip address
!
interface GigabitEthernet7/5
 no ip address
!
interface GigabitEthernet7/6
 no ip address
!
interface GigabitEthernet7/7
 no ip address
!
interface GigabitEthernet7/8
 no ip address
!
interface GigabitEthernet7/9
 no ip address
!
interface GigabitEthernet7/10
 no ip address
!
interface GigabitEthernet7/11
 no ip address
!
```

```
interface GigabitEthernet7/12
 no ip address
!
interface GigabitEthernet7/13
 no ip address
!
interface GigabitEthernet7/14
 no ip address
!
interface GigabitEthernet7/15
 no ip address
!
interface GigabitEthernet7/16
 no ip address
!
interface GigabitEthernet7/17
 description WAAS Central Manager
 switchport
 switchport access vlan 47
 switchport mode access
!
interface GigabitEthernet7/18
 no ip address
!
interface GigabitEthernet7/19
 no ip address
!
interface GigabitEthernet7/20
 no ip address
!
interface GigabitEthernet7/21
 description AW-DC-1_G1
 switchport
 switchport access vlan 43
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet7/22
 description AW-DC-2_G1
 switchport
 switchport access vlan 43
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet7/23
 description MDS Management PAME-DC-1
 switchport
 switchport access vlan 44
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet7/24
 description MDS Management MDS-DC-1_M0
 switchport
 switchport access vlan 41
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet7/25
 description MDS Management MDS-DC-2_M0
 switchport
 switchport access vlan 41
 switchport mode access
 spanning-tree portfast edge
```

```
!
interface GigabitEthernet7/26
 no ip address
!
interface GigabitEthernet7/27
 description ASA-WAN-1_M0
 switchport
 switchport access vlan 42
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet7/28
 no ip address
!
interface GigabitEthernet7/29
 description MSE-DC-1_G1
 switchport
 switchport access vlan 43
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet7/30
 description MSE-DC-2_G1
 switchport
 switchport access vlan 43
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet7/31
 no ip address
!
interface GigabitEthernet7/32
 no ip address
!
interface GigabitEthernet7/33
 description RSA enVision
 switchport
 switchport access vlan 42
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet7/34
 no ip address
!
interface GigabitEthernet7/35
 description WAE-DC-1
 switchport
 switchport access vlan 49
 switchport mode access
!
interface GigabitEthernet7/36
 no ip address
!
interface GigabitEthernet7/37
 no ip address
!
interface GigabitEthernet7/38
 no ip address
!
interface GigabitEthernet7/39
 no ip address
!
interface GigabitEthernet7/40
 no ip address
```

```
!
interface GigabitEthernet7/41
 no ip address
!
interface GigabitEthernet7/42
 no ip address
!
interface GigabitEthernet7/43
 no ip address
!
interface GigabitEthernet7/44
 no ip address
!
interface GigabitEthernet7/45
 description hard crossover bridge
 no ip address
 shutdown
!
interface GigabitEthernet7/46
 no ip address
!
interface GigabitEthernet7/47
 no ip address
 shutdown
!
interface GigabitEthernet7/48
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan803
 description ** South Side facing Servers1 **
 ip address 192.168.130.10 255.255.255.252
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 7 <removed>
 ip ospf priority 0
!
router ospf 5
 router-id 192.168.1.21
 log-adjacency-changes
 area 81 authentication message-digest
 area 81 nssa
 area 81 range 192.168.0.0 255.255.0.0
 timers throttle spf 10 100 5000
 passive-interface default
 no passive-interface Vlan803
 network 192.168.0.0 0.0.255.255 area 81
!
ip classless
no ip forward-protocol nd
!
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication CiscoACS
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Loopback0
!
logging trap debugging
```

```
logging source-interface Loopback0
logging 192.168.42.124
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps hsrp
snmp-server enable traps MAC-Notification change move threshold
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps energywise
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps port-security
snmp-server enable traps errdisable
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
!
!
control-plane
!
!
dial-peer cor custom
!
!
!
banner exec C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                  **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner incoming C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
```

```
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner login C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!


!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication CiscoACS
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
!
!
ntp source Loopback0
ntp master 5
ntp update-calendar
ntp server 171.68.10.150
ntp server 171.68.10.80 prefer
mac-address-table aging-time 480
!
end
```

RSERV-2

```
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
```

```
service sequence-numbers
service counters max age 5
!
hostname RSERV-2
!
boot-start-marker
boot-end-marker
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 50000
no logging rate-limit
enable secret 5 <removed>
!

username bart privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
aaa new-model
!
!
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
svclc module 4 vlan-group 162,163
svclc vlan-group 162  152,162
svclc vlan-group 163  153,163
intrusion-detection module 9 management-port access-vlan 42
intrusion-detection module 9 data-port 1 trunk allowed-vlan 153,154
intrusion-detection module 9 data-port 2 trunk allowed-vlan 163,164
ip wccp 61
ip wccp 62
!
!
!
no ip bootp server
ip multicast-routing
ip ssh version 2
ip scp server enable
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
ipv6 mfib hardware-switching replication-mode ingress
vtp domain CiscoCOMPLIANCE
vtp mode transparent
no mls acl tcam share-global
mls netflow interface
mls cef error action freeze
password encryption aes
!
crypto pki trustpoint TP-self-signed-1027
```

```
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1027
 revocation-check none
 rsakeypair TP-self-signed-1027
!
!
crypto pki certificate chain TP-self-signed-1027
 certificate self-signed 01
  30820241 308201AA A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  2B312930 27060355 04031320 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 31303237 301E170D 31313034 32313030 30353139 5A170D32
  30303130 31303030 3030305A 302B3129 30270603 55040313 20494F53 2D53656C
  662D5369 676E6564 2D436572 74696669 63617465 2D313032 3730819F 300D0609
  2A864886 F70D0101 01050003 818D0030 81890281 8100A365 80CA486A 1FCC3F72
  4B6DDFE1 AA57CE0A 4726554C B0D6B6F3 BC9F3F3A 84AAD96D 0C8D4E07 3E5C42FD
  2AB0BA8A 1E5E28AE BDA4FE3A F1A425A6 2D2F09E0 3DC30109 F4561A9B EADC4896
  87FD5133 4FEAFA2F C214CB35 11B7AEB6 F0C3DE4F 4453DA89 6177A6D3 9FDA59BA
  EE11414E 008C40A8 FF768B0D 0CE97204 82FB71C6 10C30203 010001A3 75307330
  0F060355 1D130101 FF040530 030101FF 30200603 551D1104 19301782 15525345
  52562D32 2E636973 636F2D69 726E2E63 6F6D301F 0603551D 23041830 16801425
  E9402754 9D8FF072 B2B9284C D1157536 23A79C30 1D060355 1D0E0416 041425E9
  4027549D 8FF072B2 B9284CD1 15753623 A79C300D 06092A86 4886F70D 01010405
  00038181 003EACB3 84C4E98F 65FE3BE2 F4984B3D 908DCF32 E89B4217 6F3444EB
  E844C491 A50B817E 508BE874 E4C1FE1E 9A92EDC5 8566CC69 AB760674 E802086B
  DDD7DF6A 3964355C 0F88B1AB 52E69373 D25A2877 3379ECAF A8D3DAE8 239C2708
  8B1C24DF 4210091C 8C3DF041 7B10147C E399480E 6A7D00DD 64D8AD86 528815E4
  7FAECE3C 2B
  quit
!
!
!
!
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
!
spanning-tree mode pvst
!
no power enable module 8
diagnostic bootup level minimal
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
redundancy
 main-cpu
  auto-sync running-config
 mode sso
!
```

```
!
vlan internal allocation policy descending
vlan dot1q tag native
vlan access-log ratelimit 2000
!
vlan 41
 name DeviceManagementHTA
!
vlan 42
 name DeviceManagement
!
vlan 43
 name WIRELESS-CONTROL
!
vlan 44
 name PhysicalSec
!
vlan 47
 name WAAS_Central_Manager
!
vlan 49
 name WAAS_DC
!
vlan 152
 name NorthSide_facing_ASA_Servers2
!
vlan 153
 name ACE_to_IDS_Servers2
!
vlan 154
 name SouthSide_facing_Servers2
!
vlan 162
 name NorthSide_facing_ASA_Servers1
!
vlan 163
 name ACE_to_IDS_Servers1
!
vlan 164
 name SouthSide_facing_Servers1
!
vlan 804
 name RSERV-2_to_RAGG-2-VDC-2
!
vlan 1000
!
!
!
!
!
interface Loopback0
 ip address 192.168.1.22 255.255.255.255
!
interface Loopback62
 ip address 192.168.62.162 255.255.255.255
!
interface GigabitEthernet1/1
 no ip address
 shutdown
!
interface GigabitEthernet1/2
 no ip address
 shutdown
!
```

```
interface GigabitEthernet1/3
 no ip address
 shutdown
!
interface GigabitEthernet1/4
 no ip address
 shutdown
!
interface GigabitEthernet1/5
 no ip address
 shutdown
!
interface GigabitEthernet1/6
 no ip address
 shutdown
!
interface GigabitEthernet1/7
 no ip address
 shutdown
!
interface GigabitEthernet1/8
 no ip address
 shutdown
!
interface GigabitEthernet1/9
 no ip address
 shutdown
!
interface GigabitEthernet1/10
 no ip address
 shutdown
!
interface GigabitEthernet1/11
 no ip address
 shutdown
!
interface GigabitEthernet1/12
 no ip address
 shutdown
!
interface GigabitEthernet1/13
 no ip address
 shutdown
!
interface GigabitEthernet1/14
 no ip address
 shutdown
!
interface GigabitEthernet1/15
 no ip address
 shutdown
!
interface GigabitEthernet1/16
 no ip address
 shutdown
!
interface TenGigabitEthernet2/1
 description to RAGG-2 vdc2 T1/15
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 162
 switchport mode trunk
!
interface TenGigabitEthernet2/2
```

```
 description to RAGG-2 vdc2 T1/16
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 152
 switchport mode trunk
!
interface TenGigabitEthernet2/3
 no ip address
 shutdown
!
interface TenGigabitEthernet2/4
 no ip address
 shutdown
!
interface TenGigabitEthernet2/5
 description to RAGG-2 vdc2 T1/18
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 41-44,164,804
 switchport mode trunk
!
interface TenGigabitEthernet2/6
 description to RAGG-2 vdc2 T1/17
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 154
 switchport mode trunk
!
interface TenGigabitEthernet2/7
 no ip address
 shutdown
!
interface TenGigabitEthernet2/8
 no ip address
 shutdown
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 no ip address
 shutdown
!
interface GigabitEthernet6/1
 no ip address
 shutdown
!
interface GigabitEthernet6/2
 no ip address
 shutdown
!
interface GigabitEthernet7/1
 switchport
 switchport access vlan 42
!
interface GigabitEthernet7/2
 no ip address
!
interface GigabitEthernet7/3
 no ip address
!
interface GigabitEthernet7/4
 no ip address
```

```
!
interface GigabitEthernet7/5
 description WAE-DC-2
 switchport
 switchport access vlan 48
 switchport mode access
!
interface GigabitEthernet7/6
 no ip address
!
interface GigabitEthernet7/7
 no ip address
!
interface GigabitEthernet7/8
 no ip address
!
interface GigabitEthernet7/9
 no ip address
!
interface GigabitEthernet7/10
 no ip address
!
interface GigabitEthernet7/11
 no ip address
!
interface GigabitEthernet7/12
 no ip address
!
interface GigabitEthernet7/13
 no ip address
!
interface GigabitEthernet7/14
 no ip address
!
interface GigabitEthernet7/15
 no ip address
!
interface GigabitEthernet7/16
 no ip address
!
interface GigabitEthernet7/17
 no ip address
!
interface GigabitEthernet7/18
 no ip address
!
interface GigabitEthernet7/19
 no ip address
!
interface GigabitEthernet7/20
 no ip address
!
interface GigabitEthernet7/21
 no ip address
!
interface GigabitEthernet7/22
 no ip address
!
interface GigabitEthernet7/23
 description PAME-DC-1
 switchport
 switchport access vlan 44
 switchport mode access
!
```

```
interface GigabitEthernet7/24
 no ip address
!
interface GigabitEthernet7/25
 no ip address
!
interface GigabitEthernet7/26
 no ip address
!
interface GigabitEthernet7/27
 description ASA-WAN-2_M0
 switchport
 switchport access vlan 42
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet7/28
 no ip address
!
interface GigabitEthernet7/29
 no ip address
!
interface GigabitEthernet7/30
 no ip address
!
interface GigabitEthernet7/31
 no ip address
!
interface GigabitEthernet7/32
 no ip address
!
interface GigabitEthernet7/33
 no ip address
!
interface GigabitEthernet7/34
 no ip address
!
interface GigabitEthernet7/35
 no ip address
!
interface GigabitEthernet7/36
 no ip address
!
interface GigabitEthernet7/37
 no ip address
!
interface GigabitEthernet7/38
 no ip address
!
interface GigabitEthernet7/39
 no ip address
!
interface GigabitEthernet7/40
 no ip address
!
interface GigabitEthernet7/41
 no ip address
!
interface GigabitEthernet7/42
 no ip address
!
interface GigabitEthernet7/43
 no ip address
!
```

```
interface GigabitEthernet7/44
 no ip address
!
interface GigabitEthernet7/45
 no ip address
!
interface GigabitEthernet7/46
 no ip address
!
interface GigabitEthernet7/47
 no ip address
!
interface GigabitEthernet7/48
 no ip address
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan42
 ip address 192.168.42.47 255.255.255.0
!
interface Vlan804
 description ** South Side facing Servers1 **
 ip address 192.168.130.14 255.255.255.252
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 7 <removed>
 ip ospf priority 0
!
router ospf 5
 router-id 192.168.1.22
 log-adjacency-changes
 area 81 authentication message-digest
 area 81 nssa
 area 81 range 192.168.0.0 255.255.0.0
 timers throttle spf 10 100 5000
 passive-interface default
 no passive-interface Vlan804
 network 192.168.0.0 0.0.255.255 area 81
!
ip classless
no ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.42.1 255 name backup_default
!
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication CiscoACS
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Loopback0
!
logging trap debugging
logging source-interface Loopback0
logging 192.168.42.124
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

```
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps hsrp
snmp-server enable traps MAC-Notification change move threshold
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps energywise
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps port-security
snmp-server enable traps errdisable
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
!
!
control-plane
!
!
dial-peer cor custom
!
!
!
banner exec C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner incoming C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
```

```
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner login C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!


!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication CiscoACS
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
!
!
ntp source Loopback0
ntp master 5
ntp update-calendar
ntp server 171.68.10.150
ntp server 171.68.10.80 prefer
mac-address-table aging-time 480
!
end
```

Access

SACCESS-1

```
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
service compress-config
service sequence-numbers
!
hostname SACCESS-1
!
boot-start-marker
```

```
boot-end-marker
!
logging snmp-authfail
logging buffered 51200 debugging
enable secret 5 <removed>
!
username bart privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
aaa new-model
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
ip subnet-zero
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
!
no ip bootp server
ip ssh version 2
ip scp server enable
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
vtp mode transparent
!
password encryption aes
!
crypto pki trustpoint TP-self-signed-112603
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-112603
 revocation-check none
 rsakeypair TP-self-signed-112603
!
!
crypto pki certificate chain TP-self-signed-112603
 certificate self-signed 01
  <removed>
  quit
!
!
power redundancy-mode redundant
archive
 log config
  logging enable
  hidekeys
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 20,41-43
!
vlan 44
 name PhysicalSec
```

```
!
vlan 45-50,52,62
!
vlan 64
 name Databases
!
vlan 72,146,164,256,666,1000
!
interface Loopback0
 no ip address
!
interface Port-channel1
 description to Aggregation Switches
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 38,41,42,44
 switchport mode trunk
 logging event link-status
 flowcontrol receive on
!
interface GigabitEthernet1/1
 description SRV-DC-1
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/2
 description SRV-DC-2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 41
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/3
 description SRV-DC-3
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/4
 description SRV-DC-4
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/5
 description SRV-DC-5
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/6
 description SRV-DC-6=CUAE
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
```

```
 spanning-tree portfast trunk
!
interface GigabitEthernet1/7
 description SRV-DC-7=CCM511
 switchport access vlan 45
 spanning-tree portfast
!
interface GigabitEthernet1/8
 description SRV-DC-8 - Oracle RDBMS 10g
 switchport access vlan 64
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 64
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/9
 description MSP-DC-1
 switchport access vlan 44
 switchport trunk encapsulation dot1q
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/10
 description SRV-DC-10
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/11
 description SRV-DC-11
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/12
 description SRV-DC-12
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/13
 description SRV-DC-13
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/14
 description SRV-DC-14
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/15
 description SRV-DC-15
```

```
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/16
 description SRV-DC-16
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/17
 description SRV-DC-17
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4094
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/18
 description SRV-DC-18
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4094
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/19
 description SRV-DC-19
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4094
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/20
 description SRV-DC-20
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4094
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/21
 description SRV-DC-21
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4094
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/22
 description SRV-DC-22
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4094
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/23
 description SRV-DC-23
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
```

```
interface GigabitEthernet1/24
 description SRV-DC-24
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/25
 description SRV-DC-25
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/26
 description server 14 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/27
 description server 15 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/28
 description server 16 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/29
 description server 18 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/30
 description server 19 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/31
 description server 20 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/32
 description server 21 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/33
 description VXML Rouer VEM
 switchport access vlan 45
 spanning-tree portfast
!
interface GigabitEthernet1/34
 description SPAN to SRV-DC-28-NICE VoiceRecorder
 switchport trunk encapsulation dot1q
 spanning-tree portfast
!
interface GigabitEthernet1/35
 description Small branch 1800 server e1
 switchport access vlan 42
```

```
 switchport trunk encapsulation dot1q
 spanning-tree portfast
!
interface GigabitEthernet1/36
 description small branch 1800 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/37
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/38
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/39
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/40
 description IPcelerate Server
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/41
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/42
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/43
 description EMC SAN Mgt-A
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/44
 description PRomise SAN M1
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
```

```
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/45
 switchport access vlan 42
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/46
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/47
 description Uplink to RSERV-1 Management G7/1
 switchport access vlan 42
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/48
 description Uplink to RSERV-2 Management G7/1
 switchport access vlan 42
 switchport mode access
 spanning-tree portfast
!
interface TenGigabitEthernet1/49
 description Uplink to RAGG-1-VDC2 T1/13
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 38,41,42,44
 switchport mode trunk
 channel-group 1 mode active
 spanning-tree portfast trunk
!
interface TenGigabitEthernet1/50
 description Uplink to RAGG-2-VDC2 T1/13
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 38,41,42,44
 switchport mode trunk
 channel-group 1 mode active
 spanning-tree portfast trunk
!
interface Vlan1
 no ip address
!
interface Vlan42
 ip address 192.168.42.33 255.255.255.0
!
no ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.42.1
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication CiscoACS
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip tacacs source-interface Vlan42
!
!
logging source-interface Vlan42
logging 192.168.42.121
access-list 23 permit 192.168.41.101 log
```

```
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access 88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFF0F
snmp-server trap-source Vlan42
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps entity
snmp-server enable traps flash insertion removal
snmp-server enable traps cpu threshold
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps port-security
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps vlan-membership
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
no tacacs-server directed-request
tacacs-server key 7 <removed>
radius-server source-ports 1645-1646
!
control-plane
!
banner exec
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                  **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner incoming
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
```

```
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner login
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!

!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication CiscoACS
 stopbits 1
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
!
!
monitor session 1 source interface Gi1/33
monitor session 1 destination interface Gi1/34
ntp clock-period 17181001
ntp server 192.168.0.1
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end
```

SACCESS-2

```
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service compress-config
service sequence-numbers
```

```
!
hostname SACCESS-2
!
boot-start-marker
boot-end-marker
!
logging buffered 51200 debugging
enable secret 5 <removed>
!
username bart privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
aaa new-model
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
aaa session-id common
clock timezone PST -8
clock summer-time PST recurring
vtp mode transparent
ip subnet-zero
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
!
no ip bootp server
ip ssh version 2
ip scp server enable
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
password encryption aes
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
power redundancy-mode redundant
!
!
!
vlan internal allocation policy ascending
!
vlan 20,40-43
!
vlan 44
 name PhysicalSec
!
vlan 45-49,52,62,64,72,146,164,256,666,1000
!
interface Port-channel2
 description to Aggregation Switches
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 38,41,42,44
 switchport mode trunk
 logging event link-status
```

```
 flowcontrol receive on
!
interface GigabitEthernet1/1
 description SRV-DC-1
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/2
 description SRV-DC-2
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/3
 description SRV-DC-3
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/4
 description SRV-DC-4
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/5
 description SRV-DC-5
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/6
 description SRV-DC-6=CUAE
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/7
 description SRV-DC-7=CCM511
 switchport access vlan 45
 spanning-tree portfast
!
interface GigabitEthernet1/8
 description SRV-DC-8
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/9
```

```
 description MSP-DC-1
 switchport access vlan 44
 switchport trunk encapsulation dot1q
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/10
 description SRV-DC-10
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/11
 description SRV-DC-11
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/12
 description SRV-DC-12
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/13
 description SRV-DC-13
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/14
 description SRV-DC-14
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/15
 description SRV-DC-15
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/16
 description SRV-DC-16
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/17
 description SRV-DC-17
```

```
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4094
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/18
 description SRV-DC-18
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4094
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/19
 description SRV-DC-19
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4094
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/20
 description SRV-DC-20
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4094
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/21
 description SRV-DC-21
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4094
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/22
 description SRV-DC-22
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4094
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/23
 description SRV-DC-23
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/24
 description SRV-DC-24
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/25
 description SRV-DC-25
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
```

```
interface GigabitEthernet1/26
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/27
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/28
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/29
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/30
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/31
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/32
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/33
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/34
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/35
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/36
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/37
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/38
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/39
 switchport access vlan 42
 switchport trunk encapsulation dot1q
```

```
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/40
 description IPcelerate Server
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/41
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/42
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/43
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/44
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/45
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet1/46
 switchport access vlan 42
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 42
 switchport mode trunk
 shutdown
 spanning-tree portfast trunk
!
interface GigabitEthernet1/47
 description TEMP Uplink to RSERV-1 Management G7/2
 switchport access vlan 42
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/48
 description TEMP Uplink to RSERV-2 Management G7/2
 switchport access vlan 42
```

```
 switchport mode access
 spanning-tree portfast
!
interface TenGigabitEthernet1/49
 description Uplink to RAGG-1-VDC2 T1/14
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 38,41,42,44
 switchport mode trunk
 spanning-tree portfast trunk
 channel-group 2 mode active
!
interface TenGigabitEthernet1/50
 description Uplink to RAGG-2-VDC2 T1/14
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 38,41,42,44
 switchport mode trunk
 spanning-tree portfast trunk
 channel-group 2 mode active
!
interface Vlan1
 no ip address
!
interface Vlan42
 ip address 192.168.42.34 255.255.255.0
!
no ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.42.1
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication CiscoACS
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Vlan42
!
!
logging trap debugging
logging source-interface Vlan42
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access 88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
snmp-server trap-source Vlan42
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps vtp
```

```
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps flash insertion removal
snmp-server enable traps syslog
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps hsrp
snmp-server enable traps vlan-membership
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
radius-server source-ports 1645-1646
banner exec
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner incoming
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner login
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!

!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication CiscoACS
 stopbits 1
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
```

```
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
!
ntp clock-period 17181029
ntp source Vlan42
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
!
end
```

SACCESS-3

```
version 5.0(3)N1(1b)
feature fcoe

feature privilege
no feature telnet
no telnet server enable
feature tacacs+
cfs eth distribute
feature lacp
feature vpc
feature lldp
feature fex

username bart password 5 <removed>  role network-admin
username bmcgloth password 5 <removed>  role network-admin
enable secret 5 <removed>

banner motd #
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
#

ssh login-attempts 6

ip domain-lookup
ip domain-name cisco-irn.com
ip host SACCESS-3 192.168.41.33
tacacs-server key 7 "<removed>"
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
```

```
    server 192.168.42.131
    use-vrf management
    source-interface mgmt0
hostname SACCESS-3
ip access-list 23
  statistics per-entry
  10 permit ip 127.0.0.1/32 192.168.41.33/32
  20 permit ip 192.168.41.101/32 192.168.41.33/32
  30 permit ip 192.168.41.102/32 192.168.41.33/32
  40 permit ip 192.168.42.111/32 192.168.41.33/32
  50 permit ip 192.168.42.122/32 192.168.41.33/32
  60 permit ip 192.168.42.131/32 192.168.41.33/32
  70 permit ip 192.168.42.133/32 192.168.41.33/32
  80 permit ip 192.168.42.138/32 192.168.41.33/32
  90 permit ip 10.19.151.99/32 192.168.41.33/32
  100 deny ip any any
ip access-list 88
  statistics per-entry
  10 permit ip 192.168.42.122/32 192.168.41.33/32
  20 deny ip any any
class-map type qos class-fcoe
class-map type queuing class-all-flood
  match qos-group 2
class-map type queuing class-ip-multicast
  match qos-group 2
class-map type network-qos class-all-flood
  match qos-group 2
class-map type network-qos class-ip-multicast
  match qos-group 2
snmp-server user bart network-admin auth md5 <removed> priv <removed> localizedkey
snmp-server user bmcgloth network-admin auth md5 <removed> priv <removed> localizedkey
snmp-server host 192.168.41.101 traps version 2c public  udp-port 2162
no snmp-server enable traps entity entity_mib_change
no snmp-server enable traps entity entity_module_status_change
no snmp-server enable traps entity entity_power_status_change
no snmp-server enable traps entity entity_module_inserted
no snmp-server enable traps entity entity_module_removed
no snmp-server enable traps entity entity_unrecognised_module
no snmp-server enable traps entity entity_fan_status_change
no snmp-server enable traps rf redundancy_framework
snmp-server enable traps entity fru
ntp server 192.168.62.161 use-vrf management
ntp server 192.168.62.162 use-vrf management
aaa authentication login default group CiscoACS
aaa authentication login console group CiscoACS
aaa authorization ssh-certificate default group CiscoACS
aaa accounting default group CiscoACS
aaa authentication login error-enable

vrf context management
  ip route 0.0.0.0/0 192.168.41.1
vlan 1
vlan 36
  name DeviceMgmtHigh
vlan 37
  name DeviceMgmtLow
vlan 38
  name HyTrust
vlan 40
  name Server_iLO
vlan 41
  name ESX_Server
vlan 42
  name CoreManagement
```

```
vlan 43
  name WirelessSystems
vlan 45
vlan 52
  name POS
vlan 80-82,140-141
vlan 302
  fcoe vsan 2
vsan database
  vsan 2 name "Promise-2"
fcdomain fcid database
  vsan 2 wwn 21:00:00:1b:32:00:ab:0d fcid 0xee0000 area dynamic
  vsan 2 wwn 21:00:00:1b:32:00:70:0d fcid 0xee0100 area dynamic
  vsan 2 wwn 21:00:00:1b:32:00:33:0c fcid 0xee0200 area dynamic
  vsan 2 wwn 21:00:00:1b:32:00:5d:0d fcid 0xee0300 area dynamic
  vsan 2 wwn 21:00:00:1b:32:80:0b:10 fcid 0xee0400 area dynamic
  vsan 2 wwn 21:00:00:1b:32:80:52:10 fcid 0xee0500 area dynamic
  vsan 2 wwn 21:00:00:1b:32:80:da:0f fcid 0xee0600 area dynamic
  vsan 2 wwn 21:00:00:1b:32:00:3a:0c fcid 0xee0700 area dynamic
  vsan 2 wwn 21:00:00:1b:32:80:f1:0f fcid 0xee0800 area dynamic
  vsan 1 wwn 26:01:00:01:55:35:7e:44 fcid 0xee0000 dynamic
  vsan 2 wwn 21:00:00:1b:32:00:5e:0d fcid 0xee0900 area dynamic


interface port-channel3
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52

interface vfc513
  bind interface Ethernet1/13
  no shutdown

interface vfc514
  bind interface Ethernet1/14
  no shutdown

interface vfc515
  bind interface Ethernet1/15
  no shutdown

interface vfc516
  bind interface Ethernet1/16
  no shutdown

interface vfc517
  bind interface Ethernet1/17
  no shutdown

interface vfc518
  bind interface Ethernet1/18
  no shutdown

interface vfc519
  bind interface Ethernet1/19
  no shutdown

interface vfc520
  bind interface Ethernet1/20
  no shutdown

interface vfc521
  bind interface Ethernet1/21
  no shutdown
```

```
interface vfc522
  bind interface Ethernet1/22
  no shutdown

interface vfc523
  bind interface Ethernet1/23
  no shutdown

interface vfc524
  bind interface Ethernet1/24
  no shutdown

interface vfc525
  bind interface Ethernet1/25
  no shutdown

interface vfc526
  bind interface Ethernet1/26
  no shutdown

interface vfc527
  bind interface Ethernet1/27
  no shutdown

interface vfc528
  bind interface Ethernet1/28
  no shutdown

interface vfc529
  bind interface Ethernet1/29
  no shutdown

interface vfc530
  bind interface Ethernet1/30
  no shutdown

interface vfc531
  bind interface Ethernet1/31
  no shutdown

interface vfc532
  bind interface Ethernet1/32
  no shutdown

interface vfc505
  bind interface Ethernet1/5
  no shutdown

interface vfc506
  bind interface Ethernet1/6
  no shutdown

interface vfc507
  bind interface Ethernet1/7
  no shutdown

interface vfc508
  bind interface Ethernet1/8
  no shutdown

interface vfc509
  bind interface Ethernet1/9
  no shutdown
```

```
interface vfc510
  bind interface Ethernet1/10
  no shutdown

interface vfc511
  bind interface Ethernet1/11
  no shutdown

interface vfc512
  bind interface Ethernet1/12
  no shutdown
vsan database
  vsan 2 interface vfc513
  vsan 2 interface vfc514
  vsan 2 interface vfc515
  vsan 2 interface vfc516
  vsan 2 interface vfc517
  vsan 2 interface vfc518
  vsan 2 interface vfc519
  vsan 2 interface vfc520
  vsan 2 interface vfc521
  vsan 2 interface vfc522
  vsan 2 interface vfc523
  vsan 2 interface vfc524
  vsan 2 interface vfc525
  vsan 2 interface vfc526
  vsan 2 interface vfc527
  vsan 2 interface vfc528
  vsan 2 interface vfc529
  vsan 2 interface vfc530
  vsan 2 interface vfc531
  vsan 2 interface vfc532
  vsan 4094 interface vfc505
  vsan 4094 interface vfc506
  vsan 4094 interface vfc507
  vsan 4094 interface vfc508
  vsan 4094 interface vfc509
  vsan 4094 interface vfc510
  vsan 2 interface vfc511
  vsan 2 interface vfc512
  vsan 2 interface fc2/1
  vsan 2 interface fc2/2
  vsan 2 interface fc2/3
  vsan 2 interface fc2/4
  vsan 2 interface fc3/1
  vsan 2 interface fc3/2
  vsan 2 interface fc3/3
  vsan 2 interface fc3/4


interface fc2/1
  switchport description Connection to MDS-DC-1
  no shutdown

interface fc2/2

interface fc2/3

interface fc2/4

interface fc3/1
  switchport description Connection to Promise 600 san
  no shutdown
```

```
interface fc3/2

interface fc3/3

interface fc3/4

interface Ethernet1/1
  description to DC-F-UCS-1 TG0/1
  switchport mode trunk
  spanning-tree port type network

interface Ethernet1/2
  description to DC-F-UCS-1 TG0/2
  switchport mode trunk
  spanning-tree port type network

interface Ethernet1/3
  description to DC-F-UCS-2 TG0/3
  switchport mode trunk
  spanning-tree port type network

interface Ethernet1/4
  description to DC-F-UCS-2 TG0/4
  switchport mode trunk
  spanning-tree port type network

interface Ethernet1/5
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/6
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/7
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/8
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/9
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/10
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/11
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/12
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/13
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/14
  switchport mode trunk
```

```
  spanning-tree port type edge trunk

interface Ethernet1/15
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/16
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/17
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/18
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/19
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/20
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/21
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/22
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/23
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/24
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/25
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/26
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/27
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/28
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/29
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/30
  switchport mode trunk
```

```
  spanning-tree port type edge trunk

interface Ethernet1/31
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/32
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/33
  description to RAGG-1-VDC2 TG1/9
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  spanning-tree port type network
  channel-group 3 mode active

interface Ethernet1/34
  description to RAGG-1-VDC2 TG1/10
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  spanning-tree port type network
  channel-group 3 mode active

interface Ethernet1/35
  description to RAGG-2-VDC2 TG1/11
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  spanning-tree port type network
  channel-group 3 mode active

interface Ethernet1/36
  description to RAGG-2-VDC2 TG1/12
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  spanning-tree port type network
  channel-group 3 mode active

interface Ethernet1/37
  shutdown

interface Ethernet1/38
  shutdown

interface Ethernet1/39
  description to SACCESS-4
  shutdown

interface Ethernet1/40
  description to SACCESS-4
  shutdown

interface Ethernet2/1

interface Ethernet2/2

interface Ethernet2/3

interface Ethernet2/4

interface Ethernet3/1

interface Ethernet3/2
```

```
interface Ethernet3/3

interface Ethernet3/4

interface mgmt0
  ip address 192.168.41.33/24
clock timezone PST -8 0
clock summer-time PST 1 Sun April 02:00 5 Sun Oct 02:00 60
system default zone default-zone permit
system default zone distribute full
line console
  exec-timeout 15
line vty
  exec-timeout 15
  access-class 23 in
boot kickstart bootflash:/n5000-uk9-kickstart.5.0.3.N1.1b.bin
boot system bootflash:/n5000-uk9.5.0.3.N1.1b.bin
interface fc2/2
interface fc2/3
interface fc2/4
interface fc2/1
  switchport fcrxbbcredit 1
  switchport fcrxbbcredit 2 mode E
interface fc3/1
interface fc3/2
interface fc3/3
interface fc3/4
logging server 192.168.42.124 6
zone default-zone permit vsan 2
zoneset distribute full vsan 2
!Full Zone Database Section for vsan 2
zone name global_zone vsan 2
    member pwwn 26:00:00:01:55:35:7e:44
    member pwwn 26:02:00:01:55:35:7e:44
    member pwwn 10:00:00:00:c9:75:68:c3
    member pwwn 10:00:00:00:c9:77:92:e9
    member pwwn 10:00:00:00:c9:77:db:c3
    member pwwn 10:00:00:00:c9:77:dc:c3
    member pwwn 10:00:00:00:c9:77:dd:bc
    member pwwn 21:00:00:1b:32:00:33:0c
    member pwwn 21:00:00:1b:32:00:3a:0c
    member pwwn 21:00:00:1b:32:00:5d:0d
    member pwwn 21:00:00:1b:32:00:5e:0d
    member pwwn 21:00:00:1b:32:00:70:0d
    member pwwn 21:00:00:1b:32:00:ab:0d
    member pwwn 21:00:00:1b:32:80:0b:10
    member pwwn 21:00:00:1b:32:80:52:10
    member pwwn 21:00:00:1b:32:80:da:0f
    member pwwn 21:00:00:1b:32:80:f1:0f

zoneset name promise-2_zs vsan 2
    member global_zone

zoneset activate name promise-2_zs vsan 2
```

SACCESS-4

```
version 5.0(3)N1(1b)
feature fcoe
```

```
feature privilege
no feature telnet
no telnet server enable
feature tacacs+
cfs eth distribute
feature lacp
feature vpc
feature lldp
feature fex

username bmcgloth password 5 <removed> role network-admin
username bart password 5 <removed> role network-admin
enable secret 5 <removed>

banner motd #
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
#

ssh login-attempts 6

ip domain-lookup
ip domain-name cisco-irn.com
ip host SACCESS-4 192.168.41.34
tacacs-server key 7 "<removed>"
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
    use-vrf management
    source-interface mgmt0
switchname SACCESS-4
ip access-list 23
  statistics per-entry
  10 permit ip 127.0.0.1/32 192.168.41.34/32
  20 permit ip 192.168.41.101/32 192.168.41.34/32
  30 permit ip 192.168.41.102/32 192.168.41.34/32
  40 permit ip 192.168.42.111/32 192.168.41.34/32
  50 permit ip 192.168.42.122/32 192.168.41.34/32
  60 permit ip 192.168.42.131/32 192.168.41.34/32
  70 permit ip 192.168.42.133/32 192.168.41.34/32
  80 permit ip 192.168.42.138/32 192.168.41.34/32
  90 permit ip 10.19.151.99/32 192.168.41.34/32
  100 deny ip any any
ip access-list 88
  statistics per-entry
  10 permit ip 192.168.42.122/32 192.168.41.34/32
  20 deny ip any any
class-map type qos class-fcoe
class-map type queuing class-all-flood
  match qos-group 2
class-map type queuing class-ip-multicast
  match qos-group 2
class-map type network-qos class-all-flood
```

```
  match qos-group 2
class-map type network-qos class-ip-multicast
  match qos-group 2
snmp-server user bart network-admin auth md5 <removed> priv <removed> localizedkey
snmp-server user bmcgloth network-admin auth md5 <removed> priv <removed> localizedkey
snmp-server enable traps entity fru
no snmp-server enable traps entity entity_mib_change
no snmp-server enable traps entity entity_module_status_change
no snmp-server enable traps entity entity_power_status_change
no snmp-server enable traps entity entity_module_inserted
no snmp-server enable traps entity entity_module_removed
no snmp-server enable traps entity entity_unrecognised_module
no snmp-server enable traps entity entity_fan_status_change
no snmp-server enable traps rf redundancy_framework
aaa authentication login default group CiscoACS
aaa authentication login console group CiscoACS
aaa authorization ssh-certificate default group CiscoACS
aaa accounting default group CiscoACS
aaa authentication login error-enable

vrf context management
  ip route 0.0.0.0/0 192.168.41.1
vlan 1
vlan 36
  name DeviceMgmtHigh
vlan 37
  name DeviceMgmtLow
vlan 38
  name HyTrust
vlan 40
  name Server_iLO
vlan 41
  name ESX_Server
vlan 42
  name CoreManagement
vlan 45,80-82,141-142
vlan 402
  fcoe vsan 2
vsan database
  vsan 2
fcdomain fcid database
  vsan 2 wwn 21:01:00:1b:32:20:5e:0d fcid 0xa20000 area dynamic
  vsan 2 wwn 21:01:00:1b:32:20:ab:0d fcid 0xa20100 area dynamic
  vsan 2 wwn 21:01:00:1b:32:20:70:0d fcid 0xa20200 area dynamic
  vsan 2 wwn 21:01:00:1b:32:20:33:0c fcid 0xa20300 area dynamic
  vsan 2 wwn 21:01:00:1b:32:20:5d:0d fcid 0xa20400 area dynamic
  vsan 2 wwn 21:01:00:1b:32:a0:0b:10 fcid 0xa20500 area dynamic
  vsan 2 wwn 21:01:00:1b:32:a0:52:10 fcid 0xa20600 area dynamic
  vsan 2 wwn 21:01:00:1b:32:a0:da:0f fcid 0xa20700 area dynamic
  vsan 2 wwn 21:01:00:1b:32:a0:f1:0f fcid 0xa20800 area dynamic
  vsan 2 wwn 21:01:00:1b:32:20:3a:0c fcid 0xa20900 area dynamic


interface port-channel4
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52

interface vfc513
  bind interface Ethernet1/13
  no shutdown

interface vfc514
  bind interface Ethernet1/14
  no shutdown
```

```
interface vfc515
  bind interface Ethernet1/15
  no shutdown

interface vfc516
  bind interface Ethernet1/16
  no shutdown

interface vfc517
  bind interface Ethernet1/17
  no shutdown

interface vfc518
  bind interface Ethernet1/18
  no shutdown

interface vfc519
  bind interface Ethernet1/19
  no shutdown

interface vfc520
  bind interface Ethernet1/20
  no shutdown

interface vfc521
  bind interface Ethernet1/21
  no shutdown

interface vfc522
  bind interface Ethernet1/22
  no shutdown

interface vfc523
  bind interface Ethernet1/23
  no shutdown

interface vfc524
  bind interface Ethernet1/24
  no shutdown

interface vfc525
  bind interface Ethernet1/25
  no shutdown

interface vfc526
  bind interface Ethernet1/26
  no shutdown

interface vfc527
  bind interface Ethernet1/27
  no shutdown

interface vfc528
  bind interface Ethernet1/28
  no shutdown

interface vfc529
  bind interface Ethernet1/29
  no shutdown

interface vfc530
  bind interface Ethernet1/30
  no shutdown
```

```
interface vfc531
  bind interface Ethernet1/31
  no shutdown

interface vfc532
  bind interface Ethernet1/32
  no shutdown

interface vfc505
  bind interface Ethernet1/5
  no shutdown

interface vfc506
  bind interface Ethernet1/6
  no shutdown

interface vfc507
  bind interface Ethernet1/7
  no shutdown

interface vfc508
  bind interface Ethernet1/8
  no shutdown

interface vfc509
  bind interface Ethernet1/9
  no shutdown

interface vfc510
  bind interface Ethernet1/10
  no shutdown

interface vfc511
  bind interface Ethernet1/11
  no shutdown

interface vfc512
  bind interface Ethernet1/12
  no shutdown
vsan database
  vsan 2 interface vfc513
  vsan 2 interface vfc514
  vsan 2 interface vfc515
  vsan 2 interface vfc516
  vsan 2 interface vfc517
  vsan 2 interface vfc518
  vsan 2 interface vfc519
  vsan 2 interface vfc520
  vsan 2 interface vfc521
  vsan 2 interface vfc522
  vsan 2 interface vfc523
  vsan 2 interface vfc524
  vsan 2 interface vfc525
  vsan 2 interface vfc526
  vsan 2 interface vfc527
  vsan 2 interface vfc528
  vsan 2 interface vfc529
  vsan 2 interface vfc530
  vsan 2 interface vfc531
  vsan 2 interface vfc532
  vsan 2 interface vfc505
  vsan 2 interface vfc506
  vsan 2 interface vfc507
```

```
  vsan 2 interface vfc508
  vsan 2 interface vfc509
  vsan 2 interface vfc510
  vsan 2 interface vfc511
  vsan 2 interface vfc512
  vsan 2 interface fc3/1


interface fc2/1
  switchport description Connection to MDS-DC-1
  no shutdown

interface fc2/2

interface fc2/3

interface fc2/4

interface fc3/1
  switchport description Connection to Promise 600 san
  no shutdown

interface fc3/2

interface fc3/3

interface fc3/4

interface Ethernet1/1
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/2
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/3
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/4
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/5
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/6
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/7
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/8
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/9
  switchport mode trunk
  spanning-tree port type edge trunk
```

```
interface Ethernet1/10
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/11
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/12
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/13
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/14
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/15
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/16
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/17
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/18
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/19
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/20
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/21
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/22
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/23
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/24
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/25
  switchport mode trunk
  spanning-tree port type edge trunk
```

```
interface Ethernet1/26
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/27
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/28
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/29
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/30
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/31
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/32
  switchport mode trunk
  spanning-tree port type edge trunk

interface Ethernet1/33
  description to RAGG-2-VDC2 TG1/9
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  spanning-tree port type network
  channel-group 4 mode active

interface Ethernet1/34
  description to RAGG-2-VDC2 TG1/10
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  spanning-tree port type network
  channel-group 4 mode active

interface Ethernet1/35
  description to RAGG-1-VDC2 TG1/11
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  spanning-tree port type network
  channel-group 4 mode active

interface Ethernet1/36
  description to RAGG-1-VDC2 TG1/12
  switchport mode trunk
  switchport trunk allowed vlan 38,41-45,52
  spanning-tree port type network
  channel-group 4 mode active

interface Ethernet1/37
  shutdown

interface Ethernet1/38
  shutdown

interface Ethernet1/39
  description link to SACCESS-3
```

```
  shutdown

interface Ethernet1/40
  description link to SACCESS-3
  shutdown

interface Ethernet2/1

interface Ethernet2/2

interface Ethernet2/3

interface Ethernet2/4

interface Ethernet3/1

interface Ethernet3/2

interface Ethernet3/3

interface Ethernet3/4

interface mgmt0
  ip address 192.168.41.34/24
clock timezone PST -8 0
clock summer-time PST 1 Sun April 02:00 5 Sun Oct 02:00 60
line console
  exec-timeout 15
line vty
  exec-timeout 15
  access-class 23 in
boot kickstart bootflash:/n5000-uk9-kickstart.5.0.3.N1.1b.bin
boot system bootflash:/n5000-uk9.5.0.3.N1.1b.bin
interface fc2/1
interface fc2/2
interface fc2/3
interface fc2/4
interface fc3/1
interface fc3/2
interface fc3/3
interface fc3/4
logging server 192.168.42.124 6
zone default-zone permit vsan 2
!Full Zone Database Section for vsan 2
zone name global_zone vsan 2
zoneset name promise-2_zs vsan 2
    member global_zone
```

SACCESS-5

```
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
!
hostname SACCESS-5
```

```
!
boot-start-marker
boot-end-marker
!
logging buffered 51200
enable secret 5 <removed>
!

username bart privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
!
aaa new-model
!
!
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PST recurring
switch 1 provision ws-c3750e-48td
system mtu routing 1500
!
!
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
login block-for 1800 attempts 6 within 65535
login quiet-mode access-class 23
login on-failure log
login on-success log
!
password encryption aes
!
crypto pki trustpoint TP-self-signed-2654502656
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2654502656
 revocation-check none
 rsakeypair TP-self-signed-2654502656
!
!
crypto pki certificate chain TP-self-signed-2654502656
 certificate self-signed 01
  <removed>   quit
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
```

```
vlan dot1q tag native
!
ip ssh version 2
ip scp server enable
!
!
!
interface FastEthernet0
 no ip address
 shutdown
!
interface GigabitEthernet1/0/1
 description SRV-DC-22 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/0/2
 description SRV-DC-23 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/0/3
 description SRV-DC-24 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/0/4
 description SRV-DC-25 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/0/5
 description SRV-DC-26 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/0/6
 description SRV-DC-27 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/0/7
 description SRV-DC-28 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/0/8
 description SRV-DC-29 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/0/9
 description SRV-DC-30 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/0/10
 description SRV-DC-31 iLO
 switchport access vlan 40
 spanning-tree portfast
!
interface GigabitEthernet1/0/11
 description DC-UCSFabric-1-A Mgmt0
 switchport access vlan 41
```

```
 spanning-tree portfast
!
interface GigabitEthernet1/0/12
 description DC-UCSFabric-1-B Mgmt0
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/13
 description DC-ASA-1 Mgmt0
 switchport access vlan 42
 spanning-tree portfast
!
interface GigabitEthernet1/0/14
 description DC-ASA-2 Mgmt0
 switchport access vlan 42
 spanning-tree portfast
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
 description SRV-DC-22 ESXi
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/23
 description SRV-DC-23 ESXi
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/24
 description SRV-DC-24 ESXi
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/25
 description SRV-DC-25 ESXi
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/26
 description SRV-DC-26 ESXi
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/27
 description SRV-DC-27 ESXi
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/28
 description SRV-DC-28 ESXi
 switchport access vlan 41
```

```
 spanning-tree portfast
!
interface GigabitEthernet1/0/29
 description SRV-DC-29 ESXi
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/30
 description SRV-DC-30 ESXi
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/31
 description SRV-DC-31 ESXi
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/32
 description SRV-DC-32 ESXi
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/33
 description SRV-DC-33 ESXi
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/34
 description SRV-DC-34 ESXi
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/35
 description SRV-DC-35 ESXi
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/36
!
interface GigabitEthernet1/0/37
 description SACCESS-3 Mgmt
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/38
 description SACCESS-4 Mgmt
 switchport access vlan 41
 spanning-tree portfast
!
interface GigabitEthernet1/0/39
 description RCORE-1 Mgmt-a
 switchport access vlan 42
 spanning-tree portfast
!
interface GigabitEthernet1/0/40
 description RCORE-1 Mgmt-b
 switchport access vlan 42
 spanning-tree portfast
!
interface GigabitEthernet1/0/41
 description RCORE-2 Mgmt-a
 switchport access vlan 42
 spanning-tree portfast
!
```

```
interface GigabitEthernet1/0/42
 description RCORE-2 Mgmt-b
 switchport access vlan 42
 spanning-tree portfast
!
interface GigabitEthernet1/0/43
!
interface GigabitEthernet1/0/44
!
interface GigabitEthernet1/0/45
!
interface GigabitEthernet1/0/46
!
interface GigabitEthernet1/0/47
 description Uplink to RAGG-2-vdc2 T2/13
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/48
 description Uplink to RAGG-1-vdc2 T2/13
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/49
!
interface GigabitEthernet1/0/50
!
interface GigabitEthernet1/0/51
!
interface GigabitEthernet1/0/52
!
interface TenGigabitEthernet1/0/1
!
interface TenGigabitEthernet1/0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan41
 ip address 192.168.41.222 255.255.255.0
!
interface Vlan42
 ip address 192.168.42.30 255.255.255.0
!
interface Vlan1000
 no ip address
!
ip default-gateway 192.168.42.1
ip classless
no ip forward-protocol nd
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication CiscoACS
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Vlan42
!
!
ip sla enable reaction-alerts
logging trap debugging
logging source-interface Vlan42
```

```
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFF0F
snmp-server trap-source Vlan42
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps energywise
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps power-ethernet group 1-4
snmp-server enable traps power-ethernet police
snmp-server enable traps cpu threshold
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps errdisable
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131 timeout 5
tacacs-server directed-request
tacacs-server key 7 <removed>
!
banner exec
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
```

```
banner incoming
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner login
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!

!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication CiscoACS
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
!
ntp clock-period 36029147
ntp source Vlan42
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end
```

Storage

MDS-DC-1-RUNNING

```
version 5.0(1a)
system default switchport mode F
feature npiv
feature privilege
feature tacacs+
role name default-role
  description This is a system defined role and applies to all users.
```

```
  rule 5 permit show feature environment
  rule 4 permit show feature hardware
  rule 3 permit show feature module
  rule 2 permit show feature snmp
  rule 1 permit show feature system
username bmcgloth password 5 <removed>   role network-admin
username bart password 5 <removed>   role network-admin
enable secret 5 <removed>

banner motd #WARNING:  **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
**** AUTHORIZED USERS ONLY! ****ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO
BE EXPRESS CONSENTTO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE
NECESSARYTO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR
OTHERREPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME
WITHOUTFURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHERCRIMINAL
CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAWENFORCEMENT OFFICIALS AND
PROSECUTION TO THE FULL EXTENT OF THE LAW.UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND
FEDERAL,CIVIL AND CRIMINAL LAWS.#

ssh login-attempts 6

ip domain-lookup
ip domain-name cisco-irn.com
ip host MDS-DC-1 192.168.41.51
tacacs-server key 7 "<removed>"
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
aaa group server radius radius
snmp-server user bart network-admin auth md5 <removed>  priv <removed>  localizedkey
snmp-server user bmcgloth network-admin auth md5 <removed>  priv <removed>  localizedkey
snmp-server host 192.168.41.101 traps version 2c public  udp-port 2162
snmp-server host 192.168.42.121 traps version 3 auth public
no snmp-server enable traps entity entity_mib_change
no snmp-server enable traps entity entity_module_status_change
no snmp-server enable traps entity entity_power_status_change
no snmp-server enable traps entity entity_module_inserted
no snmp-server enable traps entity entity_module_removed
no snmp-server enable traps entity entity_unrecognised_module
no snmp-server enable traps entity entity_fan_status_change
no snmp-server enable traps entity entity_power_out_change
no snmp-server enable traps rf redundancy_framework
ntp server 192.168.62.161
ntp server 192.168.62.162
aaa authentication login default group CiscoACS
aaa authentication login console group CiscoACS
aaa authorization ssh-certificate default group CiscoACS
aaa accounting default group CiscoACS
aaa authentication login error-enable
ip access-list 23 permit ip 127.0.0.1 0.0.0.0 192.168.41.51 0.0.0.0
ip access-list 23 permit ip 192.168.41.101 0.0.0.0 192.168.41.51 0.0.0.0
ip access-list 23 permit ip 192.168.41.102 0.0.0.0 192.168.41.51 0.0.0.0
ip access-list 23 permit ip 192.168.42.111 0.0.0.0 192.168.41.51 0.0.0.0
ip access-list 23 permit ip 192.168.42.121 0.0.0.0 192.168.41.51 0.0.0.0
ip access-list 23 permit ip 192.168.42.122 0.0.0.0 192.168.41.51 0.0.0.0
ip access-list 23 permit ip 192.168.42.131 0.0.0.0 192.168.41.51 0.0.0.0
ip access-list 23 permit ip 192.168.42.133 0.0.0.0 192.168.41.51 0.0.0.0
ip access-list 23 permit ip 192.168.42.138 0.0.0.0 192.168.41.51 0.0.0.0
ip access-list 23 permit ip 10.19.151.99 0.0.0.0 192.168.41.51 0.0.0.0
ip access-list 23 deny ip any any log-deny
vsan database
  vsan 2 name "Promise-2"
  vsan 10 name "UIM_VSAN_A_10"
fcdomain fcid database
```

```
vsan 1 wwn 50:00:40:20:03:fc:44:6a fcid 0x020000 dynamic
vsan 1 wwn 50:00:40:21:03:fc:44:6a fcid 0x020001 dynamic
vsan 1 wwn 21:00:00:e0:8b:19:70:09 fcid 0x020100 area dynamic
vsan 1 wwn 20:89:00:05:30:00:99:de fcid 0x020200 area dynamic
vsan 1 wwn 20:8a:00:05:30:00:99:de fcid 0x020300 area dynamic
vsan 1 wwn 23:00:00:05:30:00:99:e0 fcid 0x020002 dynamic
vsan 1 wwn 23:01:00:05:30:00:99:e0 fcid 0x020003 dynamic
vsan 1 wwn 23:02:00:05:30:00:99:e0 fcid 0x020004 dynamic
vsan 1 wwn 23:03:00:05:30:00:99:e0 fcid 0x020005 dynamic
vsan 1 wwn 23:04:00:05:30:00:99:e0 fcid 0x020006 dynamic
vsan 1 wwn 23:05:00:05:30:00:99:e0 fcid 0x020007 dynamic
vsan 1 wwn 23:06:00:05:30:00:99:e0 fcid 0x020008 dynamic
vsan 1 wwn 23:07:00:05:30:00:99:e0 fcid 0x020009 dynamic
vsan 1 wwn 23:08:00:05:30:00:99:e0 fcid 0x02000a dynamic
vsan 1 wwn 22:02:00:05:30:00:99:e0 fcid 0x02000b dynamic
vsan 1 wwn 22:04:00:05:30:00:99:e0 fcid 0x02000c dynamic
vsan 1 wwn 22:06:00:05:30:00:99:e0 fcid 0x02000d dynamic
vsan 1 wwn 22:08:00:05:30:00:99:e0 fcid 0x02000e dynamic
vsan 1 wwn 22:0a:00:05:30:00:99:e0 fcid 0x02000f dynamic
vsan 1 wwn 22:0c:00:05:30:00:99:e0 fcid 0x020010 dynamic
vsan 1 wwn 10:00:00:00:c9:60:df:80 fcid 0x020011 dynamic
vsan 1 wwn 23:12:00:05:30:00:99:e0 fcid 0x020012 dynamic
vsan 1 wwn 23:13:00:05:30:00:99:e0 fcid 0x020013 dynamic
vsan 1 wwn 23:14:00:05:30:00:99:e0 fcid 0x020014 dynamic
vsan 1 wwn 23:15:00:05:30:00:99:e0 fcid 0x020015 dynamic
vsan 1 wwn 23:17:00:05:30:00:99:e0 fcid 0x020016 dynamic
vsan 1 wwn 23:16:00:05:30:00:99:e0 fcid 0x020017 dynamic
vsan 1 wwn 23:18:00:05:30:00:99:e0 fcid 0x020018 dynamic
vsan 1 wwn 23:19:00:05:30:00:99:e0 fcid 0x020019 dynamic
vsan 1 wwn 11:00:00:00:00:00:00:01 fcid 0x02001a dynamic
vsan 1 wwn 20:00:00:00:00:00:00:01 fcid 0x02001b dynamic
vsan 1 wwn 10:00:00:00:c9:77:94:21 fcid 0x02001c dynamic
vsan 1 wwn 10:00:00:00:c9:77:92:e9 fcid 0x02001d dynamic
vsan 1 wwn 10:00:00:00:c9:77:dd:bc fcid 0x02001e dynamic
vsan 1 wwn 20:41:00:05:9b:73:10:c0 fcid 0x02001f dynamic
vsan 1 wwn 20:41:00:05:9b:73:17:40 fcid 0x020020 dynamic
vsan 1 wwn 10:00:00:00:c9:77:dc:c3 fcid 0x020021 dynamic
vsan 1 wwn 10:00:00:00:c9:75:68:c3 fcid 0x020022 dynamic
vsan 1 wwn 20:4c:00:0d:ec:2d:94:c0 fcid 0x020400 area dynamic
vsan 1 wwn 20:64:00:0d:ec:2d:94:c0 fcid 0x020500 area dynamic
vsan 1 wwn 10:00:00:00:c9:77:db:c3 fcid 0x020023 dynamic
vsan 2 wwn 20:4c:00:0d:ec:2d:94:c0 fcid 0xef0000 area dynamic
vsan 2 wwn 10:00:00:00:c9:75:68:c3 fcid 0xef0100 dynamic
vsan 2 wwn 10:00:00:00:c9:77:dc:c3 fcid 0xef0101 dynamic
vsan 2 wwn 10:00:00:00:c9:77:dd:bc fcid 0xef0102 dynamic
vsan 2 wwn 10:00:00:00:c9:77:db:c3 fcid 0xef0103 dynamic
vsan 2 wwn 10:00:00:00:c9:77:92:e9 fcid 0xef0104 dynamic
vsan 2 wwn 50:06:01:60:46:e0:33:aa fcid 0xef01ef dynamic
vsan 2 wwn 20:41:00:05:9b:73:10:c0 fcid 0xef0105 dynamic
vsan 1 wwn 50:06:01:68:46:e0:33:aa fcid 0x0200ef dynamic
vsan 1 wwn 50:06:01:60:46:e0:33:aa fcid 0x0206ef dynamic
vsan 2 wwn 20:41:00:05:9b:73:17:40 fcid 0xef0106 dynamic
vsan 2 wwn 10:00:00:00:c9:77:94:21 fcid 0xef0107 dynamic
vsan 2 wwn 20:64:00:0d:ec:2d:94:c0 fcid 0xef0200 area dynamic
vsan 2 wwn 50:06:01:68:46:e0:33:aa fcid 0xef03ef dynamic
vsan 10 wwn 50:06:01:60:46:e0:33:aa fcid 0xd800ef dynamic
vsan 10 wwn 20:41:00:05:9b:73:10:c0 fcid 0xd80000 dynamic
vsan 10 wwn 20:41:00:05:9b:73:17:40 fcid 0xd80001 dynamic
vsan 10 wwn 10:00:00:00:c9:77:94:21 fcid 0xd80002 dynamic
vsan 10 wwn 50:06:01:61:46:e0:33:aa fcid 0xd801ef dynamic
vsan 10 wwn 50:06:01:69:46:e0:33:aa fcid 0xd802ef dynamic
vsan 10 wwn 20:42:00:05:9b:73:10:c0 fcid 0xd80003 dynamic
vsan 10 wwn 20:00:00:25:b5:01:11:0f fcid 0xd80004 dynamic
vsan 10 wwn 20:00:00:25:b5:01:11:18 fcid 0xd80005 dynamic
```

```
  vsan 10 wwn 20:00:00:25:b5:01:11:12 fcid 0xd80006 dynamic
  vsan 10 wwn 20:00:00:25:b5:01:11:15 fcid 0xd80007 dynamic
  vsan 10 wwn 20:00:00:25:b5:01:11:19 fcid 0xd80008 dynamic
  vsan 10 wwn 20:00:00:25:b5:01:11:10 fcid 0xd80009 dynamic
  vsan 10 wwn 20:00:00:25:b5:01:11:1c fcid 0xd8000a dynamic
  vsan 10 wwn 20:00:00:25:b5:01:11:25 fcid 0xd8000b dynamic
  vsan 10 wwn 20:00:00:25:b5:01:11:22 fcid 0xd8000c dynamic
  vsan 10 wwn 20:00:00:25:b5:01:11:1f fcid 0xd8000d dynamic
  vsan 10 wwn 20:00:00:25:b5:01:11:2b fcid 0xd8000e dynamic
  vsan 10 wwn 20:00:00:25:b5:01:11:28 fcid 0xd8000f dynamic
vsan database
  vsan 2 interface fc2/1
  vsan 2 interface fc2/2
  vsan 2 interface fc2/3
  vsan 2 interface fc2/4
  vsan 2 interface fc2/5
  vsan 2 interface fc2/6
  vsan 2 interface fc2/7
  vsan 2 interface fc2/8
  vsan 2 interface fc2/9
  vsan 2 interface fc2/10
  vsan 2 interface fc2/11
  vsan 2 interface fc2/12
  vsan 2 interface fc2/13
  vsan 2 interface fc2/14
  vsan 2 interface fc2/15
  vsan 2 interface fc2/16
  vsan 2 interface fc2/17
  vsan 2 interface fc2/18
  vsan 2 interface fc2/19
  vsan 2 interface fc2/20
  vsan 2 interface fc2/21
  vsan 2 interface fc2/22
  vsan 2 interface fc2/23
  vsan 10 interface fc2/24
  vsan 10 interface fc2/25
  vsan 10 interface fc2/26
  vsan 2 interface fc2/27
  vsan 2 interface fc2/28
  vsan 2 interface fc2/29
  vsan 2 interface fc2/30
  vsan 2 interface fc2/31
  vsan 2 interface fc2/32
  vsan 2 interface fc2/33
  vsan 2 interface fc2/34
  vsan 2 interface fc2/35
  vsan 2 interface fc2/36
  vsan 2 interface fc2/37
  vsan 2 interface fc2/38
  vsan 2 interface fc2/39
  vsan 2 interface fc2/40
  vsan 2 interface fc2/41
  vsan 2 interface fc2/42
  vsan 2 interface fc2/43
  vsan 2 interface fc2/44
  vsan 2 interface fc2/45
  vsan 2 interface fc2/46
  vsan 2 interface fc2/47
  vsan 10 interface fc2/48
  vsan 2 interface fc4/1
  vsan 2 interface fc4/2
  vsan 2 interface fc4/3
  vsan 2 interface fc4/4
  vsan 2 interface fc4/5
```

```
  vsan 2 interface fc4/6
  vsan 2 interface fc4/7
  vsan 2 interface fc4/8
  vsan 2 interface fc4/9
  vsan 2 interface fc4/10
  vsan 2 interface fc4/11
  vsan 2 interface fc4/12
  vsan 2 interface fc4/13
  vsan 2 interface fc4/14
  vsan 2 interface fc4/15
  vsan 2 interface fc4/16
  vsan 2 interface fc4/17
  vsan 2 interface fc4/18
clock timezone PST -8 0
clock summer-time PST 1 Sun April 02:00 5 Sun Oct 02:00 60
ip default-gateway 192.168.41.1
switchname MDS-DC-1
line vty
  exec-timeout 15
line console
  exec-timeout 15
boot kickstart bootflash:/m9500-sf2ek9-kickstart-mzg.5.0.1a.bin.S4 sup-1
boot system bootflash:/m9500-sf2ek9-mzg.5.0.1a.bin.S4 sup-1
boot kickstart bootflash:/m9500-sf2ek9-kickstart-mzg.5.0.1a.bin.S4 sup-2
boot system bootflash:/m9500-sf2ek9-mzg.5.0.1a.bin.S4 sup-2
interface fc2/12
  switchport speed 4000
  switchport rate-mode shared
interface fc2/11
  switchport rate-mode dedicated
interface fc2/36
  switchport rate-mode dedicated
interface fc2/1
interface fc2/2
interface fc2/3
interface fc2/4
interface fc2/5
interface fc2/6
interface fc2/7
interface fc2/8
interface fc2/9
interface fc2/10
interface fc2/12
  switchport mode FL
interface fc2/13
interface fc2/14
interface fc2/15
interface fc2/16
interface fc2/17
interface fc2/18
interface fc2/19
interface fc2/20
interface fc2/21
interface fc2/22
interface fc2/23
interface fc2/24
interface fc2/25
interface fc2/26
interface fc2/27
interface fc2/28
interface fc2/29
interface fc2/30
interface fc2/31
interface fc2/32
```

```
interface fc2/33
interface fc2/34
interface fc2/35
interface fc2/37
interface fc2/38
interface fc2/39
interface fc2/40
interface fc2/41
interface fc2/42
interface fc2/43
interface fc2/44
interface fc2/45
interface fc2/46
interface fc2/47
interface fc2/48
interface fc2/11
  switchport mode auto
interface fc2/36
  switchport mode auto
interface fc4/1
interface fc4/2
interface fc4/3
interface fc4/4
interface fc4/5
interface fc4/6
interface fc4/7
interface fc4/8
interface fc4/9
interface fc4/10
interface fc4/11
interface fc4/12
interface fc4/13
interface fc4/14
interface fc4/15
interface fc4/16
interface fc4/17
interface fc4/18
logging server 192.168.42.121
logging server 192.168.42.124 6
system default zone default-zone permit
system default zone distribute full
zone default-zone permit vsan 2
zone default-zone permit vsan 10
zoneset distribute full vsan 1-2
zoneset distribute full vsan 10
!Full Zone Database Section for vsan 2
zone name global_zone vsan 2
    member pwwn 26:00:00:01:55:35:7e:44
    member pwwn 26:02:00:01:55:35:7e:44
    member pwwn 10:00:00:00:c9:75:68:c3
    member pwwn 10:00:00:00:c9:77:92:e9
    member pwwn 10:00:00:00:c9:77:db:c3
    member pwwn 10:00:00:00:c9:77:dc:c3
    member pwwn 10:00:00:00:c9:77:dd:bc
    member pwwn 21:00:00:1b:32:00:33:0c
    member pwwn 21:00:00:1b:32:00:3a:0c
    member pwwn 21:00:00:1b:32:00:5d:0d
    member pwwn 21:00:00:1b:32:00:5e:0d
    member pwwn 21:00:00:1b:32:00:70:0d
    member pwwn 21:00:00:1b:32:00:ab:0d
    member pwwn 21:00:00:1b:32:80:0b:10
    member pwwn 21:00:00:1b:32:80:52:10
    member pwwn 21:00:00:1b:32:80:da:0f
    member pwwn 21:00:00:1b:32:80:f1:0f
```

```
zoneset name promise-2_zs vsan 2
    member global_zone

zoneset activate name promise-2_zs vsan 2
!Full Zone Database Section for vsan 10
zone name UIM_20000025B5011112_5006016046E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:12
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011110_5006016046E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:10
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011112_5006016946E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:12
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011110_5006016946E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:10
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011112_5006016846E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:12
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011110_5006016846E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:10
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011112_5006016146E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:12
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011110_5006016146E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:10
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011115_5006016846E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:15
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011116_5006016846E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:16
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011115_5006016146E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:15
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011116_5006016146E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:16
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011115_5006016946E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:15
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011116_5006016946E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:16
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011115_5006016046E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:15
```

```
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011116_5006016046E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:16
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B501111A_5006016946E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:1a
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011119_5006016946E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:19
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B501111A_5006016146E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:1a
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011119_5006016146E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:19
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B501111A_5006016846E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:1a
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011119_5006016846E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:19
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B501111A_5006016046E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:1a
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011119_5006016046E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:19
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B501111D_5006016146E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:1d
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B501111C_5006016146E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:1c
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B501111D_5006016846E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:1d
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B501111C_5006016846E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:1c
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B501111D_5006016946E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:1d
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B501111C_5006016946E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:1c
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B501111D_5006016046E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:1d
```

```
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B501111C_5006016046E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:1c
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B501111F_5006016146E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:1f
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011120_5006016146E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:20
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B501111F_5006016946E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:1f
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011120_5006016946E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:20
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B501111F_5006016846E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:1f
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011120_5006016846E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:20
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B501111F_5006016046E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:1f
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011120_5006016046E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:20
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011123_5006016946E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:23
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011122_5006016946E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:22
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011123_5006016146E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:23
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011122_5006016146E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:22
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011123_5006016846E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:23
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011122_5006016846E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:22
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011123_5006016046E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:23
```

```
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011122_5006016046E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:22
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011125_5006016146E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:25
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011126_5006016146E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:26
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011125_5006016946E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:25
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011126_5006016946E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:26
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011125_5006016846E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:25
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011126_5006016846E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:26
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011125_5006016046E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:25
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011126_5006016046E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:26
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011129_5006016846E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:29
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011128_5006016846E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:28
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011129_5006016046E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:29
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011128_5006016046E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:28
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011129_5006016146E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:29
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011128_5006016146E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:28
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011129_5006016946E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:29
```

```
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011128_5006016946E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:28
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B501112B_5006016946E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:2b
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B501112C_5006016946E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:2c
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B501112B_5006016846E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:2b
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B501112C_5006016846E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:2c
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B501112B_5006016046E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:2b
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B501112C_5006016046E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:2c
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B501112B_5006016146E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:2b
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B501112C_5006016146E033AA vsan 10
    member pwwn 20:00:00:25:b5:01:11:2c
    member pwwn 50:06:01:61:46:e0:33:aa

zoneset name UIM_ZONESET_A vsan 10
    member UIM_20000025B5011112_5006016046E033AA
    member UIM_20000025B5011110_5006016046E033AA
    member UIM_20000025B5011112_5006016946E033AA
    member UIM_20000025B5011110_5006016946E033AA
    member UIM_20000025B5011112_5006016846E033AA
    member UIM_20000025B5011110_5006016846E033AA
    member UIM_20000025B5011112_5006016146E033AA
    member UIM_20000025B5011110_5006016146E033AA
    member UIM_20000025B5011115_5006016846E033AA
    member UIM_20000025B5011116_5006016846E033AA
    member UIM_20000025B5011115_5006016146E033AA
    member UIM_20000025B5011116_5006016146E033AA
    member UIM_20000025B5011115_5006016946E033AA
    member UIM_20000025B5011116_5006016946E033AA
    member UIM_20000025B5011115_5006016046E033AA
    member UIM_20000025B5011116_5006016046E033AA
    member UIM_20000025B501111A_5006016946E033AA
    member UIM_20000025B5011119_5006016946E033AA
    member UIM_20000025B501111A_5006016146E033AA
    member UIM_20000025B5011119_5006016146E033AA
    member UIM_20000025B501111A_5006016846E033AA
    member UIM_20000025B5011119_5006016846E033AA
    member UIM_20000025B501111A_5006016046E033AA
    member UIM_20000025B5011119_5006016046E033AA
    member UIM_20000025B501111D_5006016146E033AA
```

```
        member UIM_20000025B501111C_5006016146E033AA
        member UIM_20000025B501111D_5006016846E033AA
        member UIM_20000025B501111C_5006016846E033AA
        member UIM_20000025B501111D_5006016946E033AA
        member UIM_20000025B501111C_5006016946E033AA
        member UIM_20000025B501111D_5006016046E033AA
        member UIM_20000025B501111C_5006016046E033AA
        member UIM_20000025B501111F_5006016146E033AA
        member UIM_20000025B5011120_5006016146E033AA
        member UIM_20000025B501111F_5006016946E033AA
        member UIM_20000025B5011120_5006016946E033AA
        member UIM_20000025B501111F_5006016846E033AA
        member UIM_20000025B5011120_5006016846E033AA
        member UIM_20000025B501111F_5006016046E033AA
        member UIM_20000025B5011120_5006016046E033AA
        member UIM_20000025B5011123_5006016946E033AA
        member UIM_20000025B5011122_5006016946E033AA
        member UIM_20000025B5011123_5006016146E033AA
        member UIM_20000025B5011122_5006016146E033AA
        member UIM_20000025B5011123_5006016846E033AA
        member UIM_20000025B5011122_5006016846E033AA
        member UIM_20000025B5011123_5006016046E033AA
        member UIM_20000025B5011122_5006016046E033AA
        member UIM_20000025B5011125_5006016146E033AA
        member UIM_20000025B5011126_5006016146E033AA
        member UIM_20000025B5011125_5006016946E033AA
        member UIM_20000025B5011126_5006016946E033AA
        member UIM_20000025B5011125_5006016846E033AA
        member UIM_20000025B5011126_5006016846E033AA
        member UIM_20000025B5011125_5006016046E033AA
        member UIM_20000025B5011126_5006016046E033AA
        member UIM_20000025B5011129_5006016846E033AA
        member UIM_20000025B5011128_5006016846E033AA
        member UIM_20000025B5011129_5006016046E033AA
        member UIM_20000025B5011128_5006016046E033AA
        member UIM_20000025B5011129_5006016146E033AA
        member UIM_20000025B5011128_5006016146E033AA
        member UIM_20000025B5011129_5006016946E033AA
        member UIM_20000025B5011128_5006016946E033AA
        member UIM_20000025B501112B_5006016946E033AA
        member UIM_20000025B501112C_5006016946E033AA
        member UIM_20000025B501112B_5006016846E033AA
        member UIM_20000025B501112C_5006016846E033AA
        member UIM_20000025B501112B_5006016046E033AA
        member UIM_20000025B501112C_5006016046E033AA
        member UIM_20000025B501112B_5006016146E033AA
        member UIM_20000025B501112C_5006016146E033AA

    zoneset activate name UIM_ZONESET_A vsan 10

    interface fc2/1

    interface fc2/2

    interface fc2/3

    interface fc2/4

    interface fc2/5

    interface fc2/6

    interface fc2/7
```

```
interface fc2/8

interface fc2/9

interface fc2/10

interface fc2/11
  no shutdown

interface fc2/12
  no shutdown

interface fc2/13

interface fc2/14

interface fc2/15

interface fc2/16

interface fc2/17

interface fc2/18

interface fc2/19

interface fc2/20

interface fc2/21

interface fc2/22

interface fc2/23

interface fc2/24
  no shutdown

interface fc2/25
  no shutdown

interface fc2/26
  no shutdown

interface fc2/27

interface fc2/28

interface fc2/29

interface fc2/30

interface fc2/31

interface fc2/32

interface fc2/33

interface fc2/34

interface fc2/35

interface fc2/36
  no shutdown
```

```
interface fc2/37
  shutdown

interface fc2/38

interface fc2/39

interface fc2/40

interface fc2/41

interface fc2/42

interface fc2/43

interface fc2/44

interface fc2/45

interface fc2/46

interface fc2/47

interface fc2/48
  no shutdown

interface fc4/1

interface fc4/2

interface fc4/3

interface fc4/4

interface fc4/5

interface fc4/6

interface fc4/7

interface fc4/8

interface fc4/9

interface fc4/10

interface fc4/11

interface fc4/12

interface fc4/13

interface fc4/14

interface fc4/15

interface fc4/16

interface fc4/17

interface fc4/18

interface GigabitEthernet4/1
```

```
interface GigabitEthernet4/2

interface GigabitEthernet4/3

interface GigabitEthernet4/4

interface mgmt0
  ip address 192.168.41.51 255.255.255.0
  ip access-group 23 in
no system default switchport shutdown
```

MDS-DC-2-RUNNING

```
version 5.0(4)
system default switchport mode F
feature npiv
feature privilege
feature tacacs+
role name default-role
  description This is a system defined role and applies to all users.
  rule 5 permit show feature environment
  rule 4 permit show feature hardware
  rule 3 permit show feature module
  rule 2 permit show feature snmp
  rule 1 permit show feature system
username bmcgloth password 5 <removed>   role network-admin
username bart password 5 <removed>   role network-admin
enable secret 5 <removed>

banner motd #
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                  **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
#

ssh login-attempts 6

ip domain-lookup
ip domain-name cisco-irn.com
ip host MDS-DC-2 192.168.41.52
ip host MDS-DC-2 192.168.41.52
tacacs-server key 7 "<removed>"
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
aaa group server radius radius
snmp-server user bart network-admin auth md5 <removed>  priv <removed> localizedkey
snmp-server user bmcgloth network-admin auth md5 <removed> localizedkey
snmp-server host 192.168.41.101 traps version 2c public  udp-port 2162
snmp-server host 192.168.42.121 traps version 3 auth public
```

```
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO
ntp server 192.168.62.161
ntp server 192.168.62.162
aaa authentication login default group CiscoACS
aaa authentication login console group CiscoACS
aaa authorization ssh-certificate default group CiscoACS
aaa accounting default group CiscoACS
aaa authentication login error-enable
ip access-list 23 permit ip 127.0.0.1 0.0.0.0 192.168.41.52 0.0.0.0
ip access-list 23 permit ip 192.168.41.101 0.0.0.0 192.168.41.52 0.0.0.0
ip access-list 23 permit ip 192.168.41.102 0.0.0.0 192.168.41.52 0.0.0.0
ip access-list 23 permit ip 192.168.42.111 0.0.0.0 192.168.41.52 0.0.0.0
ip access-list 23 permit ip 192.168.42.121 0.0.0.0 192.168.41.52 0.0.0.0
ip access-list 23 permit ip 192.168.42.122 0.0.0.0 192.168.41.52 0.0.0.0
ip access-list 23 permit ip 192.168.42.131 0.0.0.0 192.168.41.52 0.0.0.0
ip access-list 23 permit ip 192.168.42.133 0.0.0.0 192.168.41.52 0.0.0.0
ip access-list 23 permit ip 192.168.42.138 0.0.0.0 192.168.41.52 0.0.0.0
ip access-list 23 permit ip 10.19.151.99 0.0.0.0 192.168.41.52 0.0.0.0
ip access-list 23 deny ip any any log-deny
vsan database
  vsan 2 name "Promise-2"
  vsan 11 name "UIM_VSAN_B_11"
fcdomain fcid database
  vsan 1 wwn 21:01:00:e0:8b:39:35:58 fcid 0x010000 area dynamic
  vsan 1 wwn 22:03:00:0d:ec:20:2b:40 fcid 0x010100 area dynamic
  vsan 11 wwn 20:41:00:05:9b:73:17:40 fcid 0xd40000 dynamic
  vsan 11 wwn 20:42:00:05:9b:73:17:40 fcid 0xd40001 dynamic
  vsan 1 wwn 21:00:00:e0:8b:19:35:58 fcid 0x010200 area dynamic
  vsan 11 wwn 50:06:01:69:46:e0:33:aa fcid 0xd400ef dynamic
  vsan 11 wwn 50:06:01:68:46:e0:33:aa fcid 0xd401ef dynamic
  vsan 1 wwn 26:01:00:01:55:35:7e:44 fcid 0x010300 dynamic
  vsan 2 wwn 26:01:00:01:55:35:7e:44 fcid 0x890000 dynamic
  vsan 2 wwn 20:64:00:0d:ec:38:76:00 fcid 0x890100 area dynamic
  vsan 11 wwn 20:00:00:25:b5:01:11:10 fcid 0xd40002 dynamic
  vsan 11 wwn 20:00:00:25:b5:01:11:19 fcid 0xd40003 dynamic
  vsan 11 wwn 20:00:00:25:b5:01:11:13 fcid 0xd40004 dynamic
  vsan 11 wwn 20:00:00:25:b5:01:11:16 fcid 0xd40005 dynamic
  vsan 11 wwn 20:00:00:25:b5:01:11:1a fcid 0xd40006 dynamic
  vsan 11 wwn 20:00:00:25:b5:01:11:12 fcid 0xd40007 dynamic
  vsan 11 wwn 20:00:00:25:b5:01:11:1d fcid 0xd40008 dynamic
  vsan 11 wwn 20:00:00:25:b5:01:11:26 fcid 0xd40009 dynamic
  vsan 11 wwn 20:00:00:25:b5:01:11:23 fcid 0xd4000a dynamic
  vsan 11 wwn 20:00:00:25:b5:01:11:20 fcid 0xd4000b dynamic
  vsan 11 wwn 20:00:00:25:b5:01:11:2c fcid 0xd4000c dynamic
  vsan 11 wwn 20:00:00:25:b5:01:11:29 fcid 0xd4000d dynamic
vsan database
  vsan 11 interface fc2/24
  vsan 11 interface fc2/25
  vsan 11 interface fc2/26
  vsan 11 interface fc2/48
clock timezone PST -8 0
clock summer-time PST 1 Sun April 02:00 5 Sun Oct 02:00 60
ip default-gateway 192.168.41.1
switchname MDS-DC-2
line vty
  session-limit 32
  exec-timeout 15
line console
  exec-timeout 15
boot kickstart bootflash:/m9500-sf2ek9-kickstart-mz.5.0.4.bin sup-1
```

```
boot system bootflash:/m9500-sf2ek9-mz.5.0.4.bin sup-1
boot kickstart bootflash:/m9500-sf2ek9-kickstart-mz.5.0.4.bin sup-2
boot system bootflash:/m9500-sf2ek9-mz.5.0.4.bin sup-2
interface fc2/1
interface fc2/2
interface fc2/3
interface fc2/4
interface fc2/5
interface fc2/6
interface fc2/7
interface fc2/8
interface fc2/9
interface fc2/10
interface fc2/11
interface fc2/12
interface fc2/13
interface fc2/14
interface fc2/15
interface fc2/16
interface fc2/17
interface fc2/18
interface fc2/19
interface fc2/20
interface fc2/21
interface fc2/22
interface fc2/23
interface fc2/24
interface fc2/25
interface fc2/26
interface fc2/27
interface fc2/28
interface fc2/29
interface fc2/30
interface fc2/31
interface fc2/32
interface fc2/33
interface fc2/34
interface fc2/35
interface fc2/36
interface fc2/37
interface fc2/38
interface fc2/39
interface fc2/40
interface fc2/41
interface fc2/42
interface fc2/43
interface fc2/44
interface fc2/45
interface fc2/46
interface fc2/47
interface fc2/48
logging server 192.168.42.121
logging server 192.168.42.124 6
system default zone default-zone permit
system default zone distribute full
zone default-zone permit vsan 2
zone default-zone permit vsan 11
zoneset distribute full vsan 1-2
zoneset distribute full vsan 11
!Full Zone Database Section for vsan 2
zone name global_zone vsan 2
zoneset name promise-2_zs vsan 2
    member global_zone
```

```
!Full Zone Database Section for vsan 11
zone name UIM_20000025B5011110_5006016946E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:10
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011112_5006016946E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:12
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011110_5006016046E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:10
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011112_5006016046E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:12
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011110_5006016146E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:10
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011112_5006016146E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:12
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011110_5006016846E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:10
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011112_5006016846E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:12
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011116_5006016046E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:16
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011115_5006016046E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:15
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011116_5006016946E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:16
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011115_5006016946E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:15
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011116_5006016846E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:16
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011115_5006016846E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:15
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011116_5006016146E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:16
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011115_5006016146E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:15
    member pwwn 50:06:01:61:46:e0:33:aa
```

```
zone name UIM_20000025B5011119_5006016146E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:19
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B501111A_5006016146E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:1a
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011119_5006016046E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:19
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B501111A_5006016046E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:1a
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011119_5006016946E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:19
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B501111A_5006016946E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:1a
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011119_5006016846E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:19
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B501111A_5006016846E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:1a
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B501111D_5006016146E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:1d
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B501111C_5006016146E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:1c
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B501111D_5006016846E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:1d
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B501111C_5006016846E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:1c
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B501111D_5006016946E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:1d
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B501111C_5006016946E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:1c
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B501111D_5006016046E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:1d
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B501111C_5006016046E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:1c
    member pwwn 50:06:01:60:46:e0:33:aa
```

```
zone name UIM_20000025B5011120_5006016846E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:20
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B501111F_5006016846E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:1f
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011120_5006016146E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:20
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B501111F_5006016146E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:1f
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011120_5006016046E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:20
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B501111F_5006016046E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:1f
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011120_5006016946E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:20
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B501111F_5006016946E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:1f
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011122_5006016946E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:22
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011123_5006016946E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:23
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011122_5006016146E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:22
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011123_5006016146E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:23
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011122_5006016046E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:22
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011123_5006016046E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:23
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011122_5006016846E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:22
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011123_5006016846E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:23
    member pwwn 50:06:01:68:46:e0:33:aa
```

```
zone name UIM_20000025B5011126_5006016846E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:26
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011125_5006016846E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:25
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011126_5006016946E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:26
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011125_5006016946E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:25
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011126_5006016146E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:26
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011125_5006016146E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:25
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011126_5006016046E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:26
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011125_5006016046E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:25
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011128_5006016946E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:28
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011129_5006016946E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:29
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B5011128_5006016046E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:28
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011129_5006016046E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:29
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B5011128_5006016146E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:28
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011129_5006016146E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:29
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B5011128_5006016846E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:28
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B5011129_5006016846E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:29
    member pwwn 50:06:01:68:46:e0:33:aa
```

```
zone name UIM_20000025B501112C_5006016046E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:2c
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B501112B_5006016046E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:2b
    member pwwn 50:06:01:60:46:e0:33:aa

zone name UIM_20000025B501112C_5006016946E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:2c
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B501112B_5006016946E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:2b
    member pwwn 50:06:01:69:46:e0:33:aa

zone name UIM_20000025B501112C_5006016846E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:2c
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B501112B_5006016846E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:2b
    member pwwn 50:06:01:68:46:e0:33:aa

zone name UIM_20000025B501112C_5006016146E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:2c
    member pwwn 50:06:01:61:46:e0:33:aa

zone name UIM_20000025B501112B_5006016146E033AA vsan 11
    member pwwn 20:00:00:25:b5:01:11:2b
    member pwwn 50:06:01:61:46:e0:33:aa

zoneset name UIM_ZONESET_B vsan 11
    member UIM_20000025B5011110_5006016946E033AA
    member UIM_20000025B5011112_5006016946E033AA
    member UIM_20000025B5011110_5006016046E033AA
    member UIM_20000025B5011112_5006016046E033AA
    member UIM_20000025B5011110_5006016146E033AA
    member UIM_20000025B5011112_5006016146E033AA
    member UIM_20000025B5011110_5006016846E033AA
    member UIM_20000025B5011112_5006016846E033AA
    member UIM_20000025B5011116_5006016046E033AA
    member UIM_20000025B5011115_5006016046E033AA
    member UIM_20000025B5011116_5006016946E033AA
    member UIM_20000025B5011115_5006016946E033AA
    member UIM_20000025B5011116_5006016846E033AA
    member UIM_20000025B5011115_5006016846E033AA
    member UIM_20000025B5011116_5006016146E033AA
    member UIM_20000025B5011115_5006016146E033AA
    member UIM_20000025B5011119_5006016146E033AA
    member UIM_20000025B501111A_5006016146E033AA
    member UIM_20000025B5011119_5006016046E033AA
    member UIM_20000025B501111A_5006016046E033AA
    member UIM_20000025B5011119_5006016946E033AA
    member UIM_20000025B501111A_5006016946E033AA
    member UIM_20000025B5011119_5006016846E033AA
    member UIM_20000025B501111A_5006016846E033AA
    member UIM_20000025B501111D_5006016146E033AA
    member UIM_20000025B501111C_5006016146E033AA
    member UIM_20000025B501111D_5006016846E033AA
    member UIM_20000025B501111C_5006016846E033AA
    member UIM_20000025B501111D_5006016946E033AA
    member UIM_20000025B501111C_5006016946E033AA
```

```
    member UIM_20000025B501111D_5006016046E033AA
    member UIM_20000025B501111C_5006016046E033AA
    member UIM_20000025B5011120_5006016846E033AA
    member UIM_20000025B501111F_5006016846E033AA
    member UIM_20000025B5011120_5006016146E033AA
    member UIM_20000025B501111F_5006016146E033AA
    member UIM_20000025B5011120_5006016046E033AA
    member UIM_20000025B501111F_5006016046E033AA
    member UIM_20000025B5011120_5006016946E033AA
    member UIM_20000025B501111F_5006016946E033AA
    member UIM_20000025B5011122_5006016946E033AA
    member UIM_20000025B5011123_5006016946E033AA
    member UIM_20000025B5011122_5006016146E033AA
    member UIM_20000025B5011123_5006016146E033AA
    member UIM_20000025B5011122_5006016046E033AA
    member UIM_20000025B5011123_5006016046E033AA
    member UIM_20000025B5011122_5006016846E033AA
    member UIM_20000025B5011123_5006016846E033AA
    member UIM_20000025B5011126_5006016846E033AA
    member UIM_20000025B5011125_5006016846E033AA
    member UIM_20000025B5011126_5006016946E033AA
    member UIM_20000025B5011125_5006016946E033AA
    member UIM_20000025B5011126_5006016146E033AA
    member UIM_20000025B5011125_5006016146E033AA
    member UIM_20000025B5011126_5006016046E033AA
    member UIM_20000025B5011125_5006016046E033AA
    member UIM_20000025B5011128_5006016946E033AA
    member UIM_20000025B5011129_5006016946E033AA
    member UIM_20000025B5011128_5006016046E033AA
    member UIM_20000025B5011129_5006016046E033AA
    member UIM_20000025B5011128_5006016146E033AA
    member UIM_20000025B5011129_5006016146E033AA
    member UIM_20000025B5011128_5006016846E033AA
    member UIM_20000025B5011129_5006016846E033AA
    member UIM_20000025B501112C_5006016046E033AA
    member UIM_20000025B501112B_5006016046E033AA
    member UIM_20000025B501112C_5006016946E033AA
    member UIM_20000025B501112B_5006016946E033AA
    member UIM_20000025B501112C_5006016846E033AA
    member UIM_20000025B501112B_5006016846E033AA
    member UIM_20000025B501112C_5006016146E033AA
    member UIM_20000025B501112B_5006016146E033AA

zoneset activate name UIM_ZONESET_B vsan 11

interface fc2/1

interface fc2/2

interface fc2/3

interface fc2/4

interface fc2/5

interface fc2/6

interface fc2/7

interface fc2/8

interface fc2/9

interface fc2/10
```

```
interface fc2/11

interface fc2/12

interface fc2/13

interface fc2/14

interface fc2/15

interface fc2/16

interface fc2/17

interface fc2/18

interface fc2/19

interface fc2/20

interface fc2/21

interface fc2/22

interface fc2/23

interface fc2/24

interface fc2/25

interface fc2/26

interface fc2/27

interface fc2/28

interface fc2/29

interface fc2/30

interface fc2/31

interface fc2/32

interface fc2/33

interface fc2/34

interface fc2/35

interface fc2/36

interface fc2/37

interface fc2/38

interface fc2/39

interface fc2/40

interface fc2/41

interface fc2/42
```

```
interface fc2/43

interface fc2/44

interface fc2/45

interface fc2/46

interface fc2/47

interface fc2/48

interface mgmt0
  ip address 192.168.41.52 255.255.255.0
  ip access-group 23 in
no system default switchport shutdown
```

Internet Edge

WAN

RIE-1

```
version 15.3
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
no platform punt-keepalive disable-kernel-core
!
hostname RIE-1
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 50000
no logging rate-limit
enable secret 4 <removed>
!
aaa new-model
```

```
!
!
aaa group server tacacs+ PRIMARY1
 server name PRIMARY
 ip tacacs source-interface GigabitEthernet0/0/1
!
aaa authentication login CiscoACS group PRIMARY1 local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default
 action-type start-stop
 group tacacs+
!
aaa accounting commands 15 default
 action-type start-stop
 group tacacs+
!
aaa accounting system default
 action-type start-stop
 group tacacs+
!
!
!
!
!
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PST recurring
!
!
!
!
!


no ip bootp server
ip domain name cisco-irn.com
ip name-server 192.168.42.130
!
!
!
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
no ipv6 source-route
ipv6 unicast-routing
ipv6 multicast rpf use-bgp
!
!
multilink bundle-name authenticated
password encryption aes
!
crypto pki trustpoint TP-self-signed-2651906707
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2651906707
 revocation-check none
 rsakeypair TP-self-signed-2651906707
!
!
crypto pki certificate chain TP-self-signed-2651906707
 certificate self-signed 01
```

```
  3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 32363531 39303637 3037301E 170D3132 31313036 31323232
  33355A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 36353139
  30363730 3730819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100AECB 6BFA1E96 248A2BFB E7B5D97E 9E9F99B1 4A2A7548 89CBC154 14CA1328
  5625CD4E 0E7F9D0F 8B0A76D7 48B1A6EB 264E67FE 70BBC476 B21A22C7 6431842D
  E5C6FBD1 3E0BBBDF 73A3088C BA6B8172 C32D446F 406F1269 0C4638D5 A422A709
  7AF6DCCE 8ACE5CD8 D686075C 46E44292 308E3E34 EFA13429 E198C0CA E8FE7300
  2A130203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF 301F0603
  551D2304 18301680 14EB092C 62224E75 39C28FA2 B39CD19D 58235B24 FB301D06
  03551D0E 04160414 EB092C62 224E7539 C28FA2B3 9CD19D58 235B24FB 300D0609
  2A864886 F70D0101 05050003 81810077 4AF3549B 69563163 6AB2398F 3068F49F
  48284235 25D42BF2 A4C45F09 17AF8EFF 5C92A80E 50AD61C8 C309E328 AE7EA370
  02CCC23E 31F1034D 69A35747 C954DFA1 0F08DB33 081F69B4 43D00153 33F03918
  68B2FD17 7070FA3C 344CB4D9 AFFE2671 3B7087F0 177F7AF2 DF3F9B1D 08144FC0
  1F42863C 4948E425 DFF1C657 1B37D6
        quit
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
!
!
!
!
!
!
username bart privilege 15 secret 4 <removed>
username bmcgloth privilege 15 secret 4 <removed>
username csmadmin privilege 15 secret 4 <removed>
username ciscolms privilege 15 secret 4 <removed>
!
redundancy
 mode none
!
!
!
ip ssh version 2
ip scp server enable
!
policy-map COPPr
 class class-default
  police 8000
!
!
!
!
!
!
!
!
interface GigabitEthernet0/0/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/1
 description link to RIE-3 G1/1
 ip address 192.168.22.11 255.255.255.0
 ip access-group INTERNAL-FILTER-IN in
 standby version 2
```

```
 standby 1 ip 192.168.22.10
 standby 1 priority 105
 standby 1 preempt
 standby 1 authentication TheCure
 standby 2 ipv6 2001:DB8:192:22::10/64
 standby 2 priority 105
 standby 2 preempt
 standby 2 authentication TheCure
 speed 1000
 no negotiation auto
 ipv6 address 2001:DB8:192:22::11/64
 ipv6 verify unicast source reachable-via rx
 ipv6 traffic-filter IPv6-INTERNAL-FILTER-IN in
!
interface GigabitEthernet0/0/2
 description link to RIE-4 G1/1
 no ip address
 shutdown
 speed 1000
 no negotiation auto
!
interface GigabitEthernet0/0/3
 description Link to RSP-3 G0/2
 ip address 10.10.3.6 255.255.255.0
 ip access-group COARSE-FILTER-INTERNET-IN in
 ip access-group COARSE-FILTER-INTERNET-OUT out
 speed 1000
 no negotiation auto
 ipv6 address 2001:DB8:1010:3::6/64
 no ipv6 redirects
 ipv6 verify unicast source reachable-via rx allow-default
 ipv6 traffic-filter IPv6-COARSE-FILTER-INTERNET-IN in
 ipv6 traffic-filter IPv6-COARSE-FILTER-INTERNET-OUT out
!
interface GigabitEthernet0/0/4
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/5
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
!
no ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.10.3.1
ip route 10.10.0.0 255.255.0.0 192.168.22.1
ip route 10.10.0.0 255.255.255.0 10.10.3.1
ip route 10.10.4.0 255.255.255.0 192.168.22.12
ip route 192.168.0.0 255.255.0.0 192.168.22.1
ip tacacs source-interface GigabitEthernet0/0/1
!
ip access-list extended COARSE-FILTER-INTERNET-IN
 remark ---Temporary LAB permit - remove from Production Network---
 permit ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
```

```
 permit ip 10.0.0.0 0.255.255.255 192.168.0.0 0.0.255.255
 permit ip 172.16.0.0 0.15.255.255 10.0.0.0 0.255.255.255
 permit ip 172.16.0.0 0.15.255.255 192.168.0.0 0.0.255.255
 remark ------------------------------------------------------
 remark ---Block Private Networks---
 deny   ip 10.0.0.0 0.255.255.255 any log
 deny   ip 172.16.0.0 0.15.255.255 any log
 deny   ip 192.168.0.0 0.0.255.255 any log
 remark -
 remark ---Block Autoconfiguration Networks---
 deny   ip 169.254.0.0 0.0.255.255 any log
 remark -
 remark ---Block Loopback Networks---
 deny   ip 127.0.0.0 0.0.255.255 any log
 remark -
 remark ---Block Multicast Networks---
 deny   ip 224.0.0.0 15.255.255.255 any log
 remark -
 remark ---Block Traffic targeted at DMZ Network Edge Devices---
 deny   ip any 192.168.22.0 0.0.0.255 log
 remark -
 remark ---Block Spoofing of your networks---
 remark enter your IP block here
 remark ---Permit all other traffic---
 permit ip any any
ip access-list extended COARSE-FILTER-INTERNET-OUT
 remark ---Block private networks from reaching Internet---
 remark ---Temporary LAB permit - remove from Production networks---
 permit ip any any
 remark ------------------------------------------------------
 remark ---Block Private Networks---
 deny   ip 10.0.0.0 0.255.255.255 any log
 deny   ip 172.16.0.0 0.15.255.255 any log
 deny   ip 192.168.0.0 0.0.255.255 any log
 remark -
 remark ---Block Autoconfiguration Networks---
 deny   ip 169.254.0.0 0.0.255.255 any log
 remark -
 remark ---Block Loopback Networks---
 deny   ip 127.0.0.0 0.0.255.255 any log
 remark -
 remark ---Block Multicast Networks---
 deny   ip 224.0.0.0 15.255.255.255 any log
 remark -
 remark ---Block Traffic targeted at DMZ Network Edge Devices---
 deny   ip any 192.168.22.0 0.0.0.255 log
 remark -
 remark ---Permit all other traffic---
 permit tcp any any
 permit udp any any
 permit icmp any any
ip access-list extended INTERNAL-FILTER-IN
 remark ------------------------------------------------------
 remark ---Permit Admin Management---
 permit icmp any any
 permit tcp host 192.168.41.101 host 192.168.22.11 eq 22 log
 permit tcp host 192.168.41.102 host 192.168.22.11 eq 22 log
 permit tcp host 192.168.42.122 host 192.168.22.11 eq 22 log
 permit tcp host 192.168.42.124 host 192.168.22.11 eq 22 log
 permit tcp host 192.168.42.131 eq tacacs host 192.168.22.11
 permit tcp host 192.168.42.133 host 192.168.22.11 eq 22 log
 permit tcp host 192.168.42.139 host 192.168.22.11 eq 22 log
 permit tcp host 10.19.151.104 host 192.168.22.11 eq 22 log
 permit tcp host 10.19.151.102 host 192.168.22.11 eq 22 log
```

```
 permit tcp host 10.19.151.103 host 192.168.22.11 eq 22 log
 permit tcp host 10.19.151.100 host 192.168.22.11 eq 22 log
 permit tcp host 10.19.151.101 host 192.168.22.11 eq 22 log
 permit tcp host 10.19.151.98 host 192.168.22.11 eq 22 log
 permit tcp host 10.19.151.99 host 192.168.22.11 eq 22 log
 permit udp host 192.168.42.122 host 192.168.22.11 eq snmp
 permit udp host 192.168.42.124 host 192.168.22.11 eq snmp
 permit udp host 192.168.42.133 host 192.168.22.11 eq snmp
 permit udp host 192.168.42.139 host 192.168.22.11 eq snmp
 remark -
 remark ---Permit HSRP V2 packets---
 permit udp host 192.168.22.12 host 224.0.0.102 eq 1985
 remark -
 remark ---Deny other connections to Edge Router---
 deny   ip any host 192.168.22.11 log
 deny   ip any host 192.168.22.10 log
 deny   ip any host 10.10.0.3 log
 remark -
 remark ---Permit all other traffic to Internet---
 permit ip any any
!
logging trap debugging
logging source-interface GigabitEthernet0/0/1
logging host 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 192.168.42.139 log
access-list 23 permit 10.19.151.104 log
access-list 23 permit 10.19.151.102 log
access-list 23 permit 10.19.151.103 log
access-list 23 permit 10.19.151.100 log
access-list 23 permit 10.19.151.101 log
access-list 23 permit 10.19.151.98 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
ipv6 route 2001:DB8:192::/48 2001:DB8:192:22::1
ipv6 route ::/0 2001:DB8:1010:3::1
!
snmp-server group V3Group v3 priv read V3Read write V3Write
snmp-server view V3Read iso included
snmp-server view V3Write iso included
snmp-server trap-source GigabitEthernet0/0/1
snmp-server packetsize 8192
snmp-server location Building SJC-17-1 Aisle 1 Rack 1
snmp-server contact Bart McGlothin
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps ipsla
snmp-server enable traps flash insertion removal
```

```
snmp-server host 192.168.42.134 version 3 priv <removed>
snmp-server host 192.168.42.139 version 3 priv <removed>
snmp-server host 192.168.42.133 version 3 priv <removed>
!
tacacs server PRIMARY
 address ipv4 192.168.42.131
 key 7 <removed>
!
!
ipv6 access-list BLOCKALL-IPv6
 deny ipv6 any any log
!
ipv6 access-list IPv6-COARSE-FILTER-INTERNET-IN
 remark ---Temporary LAB permit for use of documentation IPv6 space---
 permit ipv6 2001:DB8::/32 2001:DB8::/32
 remark ------------------------------------------------------------
 remark ---Block all traffic DHCP server -> client---
 deny udp any eq 547 any eq 546
 remark ---Block all traffic DHCP client -> server---
 deny udp any eq 546 any eq 547
 remark ---Block all traffic Routing Header Type 0---
 deny ipv6 any any routing-type 0
 remark -
 remark ---Accept all ICMPv6 packets for Neighbor Discovery and Path MTU Discovery ---
 permit icmp any any nd-na
 permit icmp any any nd-ns
 permit icmp any any router-advertisement
 permit icmp any any router-solicitation
 permit icmp any any packet-too-big
 permit icmp any any destination-unreachable
 permit icmp any any unreachable
 permit icmp any any no-route
 permit icmp any any echo-reply
 permit icmp any any echo-request
 permit icmp any any time-exceeded
 permit icmp any any parameter-problem
 permit icmp any any mld-query
 permit icmp any any mld-reduction
 permit icmp any any mld-report
 permit icmp any any port-unreachable
 remark --
 remark ---Block IETF Documentation Network---
 deny ipv6 2001:DB8::/32 any
 remark ---
 remark ---Block Spoofing of Your Networks---
 deny ipv6 2001:DB8:192::/48 any
 remark ----
 remark ---Block Traffic targeted at DMZ Network Edge Devices---
 deny ipv6 any 2001:DB8:192:22::/64 log
 remark ------
 remark ---Permit Only Assigned Networks to Your Network---
 permit ipv6 2000::/3 2001:DB8:192::/48
!
ipv6 access-list IPv6-COARSE-FILTER-INTERNET-OUT
 remark ---Temporary LAB permit for use of documentation IPv6 space---
 permit ipv6 2001:DB8::/32 2001:DB8::/32
 remark ------------------------------------------------------
 remark ---Block private networks from reaching Internet---
 remark ---Block IETF reserved Networks---
 deny ipv6 FEC0::/10 any log
 deny ipv6 FC00::/7 any log
 deny ipv6 host :: any log
 deny ipv6 ::/96 any log
 deny ipv6 ::/8 any log
```

```
 deny ipv6 ::FFFF:0.0.0.0/96 any log
 deny ipv6 2001:DB8::/32 any log
 remark -
 remark ---Block Loopback Address---
 deny ipv6 host ::1 any log
 remark --
 remark ---Block Multicast Networks---
 deny ipv6 FE00::/7 any log
 remark ---
 remark ---Alternate is to Permit Traffic From My Network to Assigned Networks---
 remark ----
 permit ipv6 2001:DB8:192::/48 2000::/3
 remark -----
 remark ---Explicit Deny for All Other Networks and Log---
 deny ipv6 any any log
!
ipv6 access-list IPv6-INTERNAL-FILTER-IN
 remark ------------------------------------------------------
 permit icmp any any
 remark -
 remark ---Permit HSRP V2 packets---
 permit udp host 2001:DB8:192:22::12 eq 2029 host FF02::66 eq 2029
 permit udp host FE80::E6D3:F1FF:FE77:A202 eq 2029 host FF02::66 eq 2029
 remark ---Deny other connections to Edge Router---
 deny ipv6 any 2001:DB8:192:22::/64 log
 remark ---Permit My Network Traffic to Assigned Networks---
 permit ipv6 2001:DB8:192::/48 2000::/3
!
control-plane
!
banner exec ^CCC
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.


UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

^C
banner incoming ^CCC
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

^C
banner login ^CCC
```

```
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!


^C
!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication CiscoACS
 stopbits 1
line aux 0
 session-timeout 1  output
 exec-timeout 0 1
 privilege level 0
 no exec
 transport preferred none
 transport output none
 stopbits 1
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 ipv6 access-class BLOCKALL-IPv6 in
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 ipv6 access-class BLOCKALL-IPv6 in
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
!
ntp source GigabitEthernet0/0/3
ntp server 171.68.10.80 prefer
ntp server 171.68.10.150
!
!
end
```

RIE-2

```
version 15.3
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
no platform punt-keepalive disable-kernel-core
!
hostname RIE-2
!
```

```
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 50000
no logging rate-limit
enable secret 4 <removed>
!
aaa new-model
!
!
aaa group server tacacs+ PRIMARY1
 server name PRIMARY
 ip tacacs source-interface GigabitEthernet0/0/2
!
aaa authentication login CiscoACS group PRIMARY1 local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default
 action-type start-stop
 group tacacs+
!
aaa accounting commands 15 default
 action-type start-stop
 group tacacs+
!
aaa accounting system default
 action-type start-stop
 group tacacs+
!
!
!
!
!
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PST recurring
!
!
!
!
!


no ip bootp server
ip domain name cisco-irn.com
ip name-server 192.168.42.130
!
!
!
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
```

```
login on-failure log
login on-success log
no ipv6 source-route
ipv6 unicast-routing
ipv6 multicast rpf use-bgp
!
!
multilink bundle-name authenticated
password encryption aes
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
!
!
username bart privilege 15 secret 4 <removed>
username bmcgloth privilege 15 secret 4 <removed>
username csmadmin privilege 15 secret 4 <removed>
username ciscolms privilege 15 secret 4 <removed>
!
redundancy
 mode none
!
!
!
ip ssh version 2
ip scp server enable
!
policy-map COPPr
 class class-default
  police 8000
!
!
!
!
!
!
!
!
interface GigabitEthernet0/0/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/1
 description link to RIE-3 G1/2
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/2
 description link to RIE-4 G1/2
 ip address 192.168.22.12 255.255.255.0
 ip access-group INTERNAL-FILTER-IN in
 standby version 2
 standby 1 ip 192.168.22.10
 standby 1 authentication TheCure
 standby 2 ipv6 2001:DB8:192:22::10/64
 standby 2 authentication TheCure
 negotiation auto
 ipv6 address 2001:DB8:192:22::12/64
```

```
 ipv6 verify unicast source reachable-via rx
 ipv6 traffic-filter IPv6-INTERNAL-FILTER-IN in
!
interface GigabitEthernet0/0/3
 description Link to RSP-4 G0/2
 ip address 10.10.4.6 255.255.255.0
 ip access-group COARSE-FILTER-INTERNET-IN in
 ip access-group COARSE-FILTER-INTERNET-OUT out
 negotiation auto
 ipv6 address 2001:DB8:1010:4::6/64
 no ipv6 redirects
 ipv6 verify unicast source reachable-via rx
 ipv6 traffic-filter IPv6-COARSE-FILTER-INTERNET-IN in
 ipv6 traffic-filter IPv6-COARSE-FILTER-INTERNET-OUT out
!
interface GigabitEthernet0/0/4
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/5
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
!
no ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.10.4.1
ip route 10.10.0.0 255.255.0.0 192.168.22.1
ip route 10.10.0.0 255.255.255.0 10.10.4.1
ip route 10.10.3.0 255.255.255.0 192.168.22.11
ip route 192.168.0.0 255.255.0.0 192.168.22.1
!
ip access-list extended COARSE-FILTER-INTERNET-IN
 remark ---Temporary LAB permit - remove from Production network---
 permit ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
 permit ip 10.0.0.0 0.255.255.255 192.168.0.0 0.0.255.255
 permit ip 172.16.0.0 0.15.255.255 10.0.0.0 0.255.255.255
 permit ip 172.16.0.0 0.15.255.255 192.168.0.0 0.0.255.255
 remark ------------------------------------------------------
 remark ---Block Private Networks---
 deny   ip 10.0.0.0 0.255.255.255 any log
 deny   ip 172.16.0.0 0.15.255.255 any log
 deny   ip 192.168.0.0 0.0.255.255 any log
 remark -
 remark ---Block Autoconfiguration Networks---
 deny   ip 169.254.0.0 0.0.255.255 any log
 remark -
 remark ---Block Loopback Networks---
 deny   ip 127.0.0.0 0.0.255.255 any log
 remark -
 remark ---Block Multicast Networks---
 deny   ip 224.0.0.0 15.255.255.255 any log
 remark -
 remark ---Block Traffic targeted at DMZ Network Edge Devices---
 deny   ip any 192.168.22.0 0.0.0.255 log
```

```
 remark -
 remark ---Block Spoofing of your networks---
 remark enter your IP block here
 deny   ip 192.168.20.0 0.0.0.255 any
 remark --
 remark ---Permit all other traffic---
 permit ip any any
ip access-list extended COARSE-FILTER-INTERNET-OUT
 remark ---Block private networks from reaching Internet---
 remark ---Temporary LAB permit - remove from Production networks---
 permit ip any any
 remark ------------------------------------------------------
 remark ---Block Private Networks---
 deny   ip 10.0.0.0 0.255.255.255 any log
 deny   ip 172.16.0.0 0.15.255.255 any log
 deny   ip 192.168.0.0 0.0.255.255 any log
 remark -
 remark ---Block Autoconfiguration Networks---
 deny   ip 169.254.0.0 0.0.255.255 any log
 remark -
 remark ---Block Loopback Networks---
 deny   ip 127.0.0.0 0.0.255.255 any log
 remark -
 remark ---Block Multicast Networks---
 deny   ip 224.0.0.0 15.255.255.255 any log
 remark -
 remark ---Block Traffic targeted at DMZ Network Edge Devices---
 deny   ip any 192.168.22.0 0.0.0.255 log
 remark -
 remark ---Permit all other traffic---
 permit tcp any any
 permit udp any any
 permit icmp any any
ip access-list extended INTERNAL-FILTER-IN
 remark ------------------------------------------------------
 remark ---Permit Admin Management---
 permit icmp any any
 permit tcp host 192.168.41.101 host 192.168.22.12 eq 22 log
 permit tcp host 192.168.41.102 host 192.168.22.12 eq 22 log
 permit tcp host 192.168.42.122 host 192.168.22.12 eq 22 log
 permit tcp host 192.168.42.124 host 192.168.22.12 eq 22 log
 permit tcp host 192.168.42.131 eq tacacs host 192.168.22.12
 permit tcp host 192.168.42.133 host 192.168.22.12 eq 22 log
 permit tcp host 192.168.42.139 host 192.168.22.12 eq 22 log
 permit tcp host 10.19.151.104 host 192.168.22.12 eq 22 log
 permit tcp host 10.19.151.102 host 192.168.22.12 eq 22 log
 permit tcp host 10.19.151.103 host 192.168.22.12 eq 22 log
 permit tcp host 10.19.151.100 host 192.168.22.12 eq 22 log
 permit tcp host 10.19.151.101 host 192.168.22.12 eq 22 log
 permit tcp host 10.19.151.98 host 192.168.22.12 eq 22 log
 permit tcp host 10.19.151.99 host 192.168.22.12 eq 22 log
 permit udp host 192.168.42.122 host 192.168.22.12 eq snmp
 permit udp host 192.168.42.124 host 192.168.22.12 eq snmp
 permit udp host 192.168.42.133 host 192.168.22.12 eq snmp
 permit udp host 192.168.42.139 host 192.168.22.12 eq snmp
 remark -
 remark ---Permit HSRP V2 packets---
 permit udp host 192.168.22.11 host 224.0.0.102 eq 1985
 remark -
 remark ---Deny other connections to Edge Router---
 deny   ip any host 192.168.22.12 log
 deny   ip any host 192.168.22.10 log
 deny   ip any host 10.10.0.3 log
 remark -
```

```
 remark ---Permit all other traffic to Internet---
 permit ip any any
!
logging trap debugging
logging source-interface GigabitEthernet0/0/2
logging host 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 192.168.42.139 log
access-list 23 permit 10.19.151.104 log
access-list 23 permit 10.19.151.102 log
access-list 23 permit 10.19.151.103 log
access-list 23 permit 10.19.151.100 log
access-list 23 permit 10.19.151.101 log
access-list 23 permit 10.19.151.98 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
ipv6 route 2001:DB8:192::/48 2001:DB8:192:22::1
ipv6 route ::/0 2001:DB8:1010:4::1
!
snmp-server group V3Group v3 priv read V3Read write V3Write
snmp-server view V3Read iso included
snmp-server view V3Write iso included
snmp-server trap-source GigabitEthernet0/0/2
snmp-server packetsize 8192
snmp-server location Building SJC-17-1 Aisle 1 Rack 1
snmp-server contact Bart McGlothin
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps ipsla
snmp-server enable traps flash insertion removal
snmp-server host 192.168.42.134 version 3 priv <removed>
snmp-server host 192.168.42.139 version 3 priv <removed>
snmp-server host 192.168.42.133 version 3 priv <removed>
!
tacacs server PRIMARY
 address ipv4 192.168.42.131
 key 7 <removed>
!
!
ipv6 access-list BLOCKALL-IPv6
 deny ipv6 any any log
!
ipv6 access-list IPv6-COARSE-FILTER-INTERNET-IN
 remark ------------------------------------------------------------
 remark ---Block all traffic DHCP server -> client---
 deny udp any eq 547 any eq 546
 remark ---Block all traffic DHCP client -> server---
 deny udp any eq 546 any eq 547
```

```
 remark ---Block all traffic Routing Header Type 0---
 deny ipv6 any any routing-type 0
 remark -
 remark ---Accept all ICMPv6 packets for Neighbor Discovery and Path MTU Discovery ---
 permit icmp any any nd-na
 permit icmp any any nd-ns
 permit icmp any any router-advertisement
 permit icmp any any router-solicitation
 permit icmp any any packet-too-big
 permit icmp any any destination-unreachable
 permit icmp any any unreachable
 permit icmp any any no-route
 permit icmp any any echo-reply
 permit icmp any any echo-request
 permit icmp any any time-exceeded
 permit icmp any any parameter-problem
 permit icmp any any mld-query
 permit icmp any any mld-reduction
 permit icmp any any mld-report
 permit icmp any any port-unreachable
 remark --
 remark ---Block IETF Documentation Network---
 remark - deny ipv6 2001:DB8::/32 any - need for Lab validation
 remark ---
 remark ---Block Spoofing of Your Networks---
 deny ipv6 2001:DB8:192::/48 any
 remark ----
 remark ---Block Traffic targeted at DMZ Network Edge Devices---
 deny ipv6 any 2001:DB8:192:22::/64 log
 remark ------
 remark ---Permit Only Assigned Networks to Your Network---
 permit ipv6 2000::/3 2001:DB8:192::/48
!
ipv6 access-list IPv6-COARSE-FILTER-INTERNET-OUT
 remark ---Temporary LAB permit for use of documentation IPv6 space---
 permit ipv6 2001:DB8::/32 2001:DB8::/32
 remark -----------------------------------------------------
 remark ---Block private networks from reaching Internet---
 remark ---Block IETF reserved Networks---
 deny ipv6 FEC0::/10 any log
 deny ipv6 FC00::/7 any log
 deny ipv6 host :: any log
 deny ipv6 ::/96 any log
 deny ipv6 ::/8 any log
 deny ipv6 ::FFFF:0.0.0.0/96 any log
 deny ipv6 2001:DB8::/32 any log
 remark -
 remark ---Block Loopback Address---
 deny ipv6 host ::1 any log
 remark --
 remark ---Block Multicast Networks---
 deny ipv6 FE00::/7 any log
 remark ---
 remark ---Alternate is to Permit Traffic From My Network to Assigned Networks---
 remark ----
 permit ipv6 2001:DB8:192::/48 2000::/3
 remark -----
 remark ---Explicit Deny for All Other Networks and Log---
 deny ipv6 any any log
!
ipv6 access-list IPv6-INTERNAL-FILTER-IN
 remark -----------------------------------------------------
 permit icmp any any
 remark -
```

```
 remark ---Permit HSRP V2 packets---
 permit udp host 2001:DB8:192:22::11 eq 2029 host FF02::66 eq 2029
 permit udp host FE80::E6D3:F1FF:FE77:D901 eq 2029 host FF02::66 eq 2029
 remark ---Deny other connections to Edge Router---
 deny ipv6 any 2001:DB8:192:22::/64 log
 remark ---Permit My Network Traffic to Assigned Networks---
 permit ipv6 2001:DB8:192::/48 2000::/3
!
control-plane
!
banner exec ^CC
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                  **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.


UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

^C
banner incoming ^CC
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                  **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

^C
banner login ^CC
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!


^C
!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication CiscoACS
 stopbits 1
line aux 0
 session-timeout 1  output
 exec-timeout 0 1
 privilege level 0
 no exec
 transport preferred none
 transport output none
 stopbits 1
line vty 0 4
```

```
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 ipv6 access-class BLOCKALL-IPv6 in
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 ipv6 access-class BLOCKALL-IPv6 in
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
!
ntp source GigabitEthernet0/0/3
ntp server 171.68.10.80 prefer
ntp server 171.68.10.150
!
!
end
```

Converged Core/Aggregation

ASA-IE-1

```
hostname ASA-IE-1
domain-name cisco-irn.com
enable password <removed> encrypted
passwd <removed> encrypted
names
dns-guard
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 192.168.21.1 255.255.255.0 standby 192.168.21.2
 ipv6 address 2001:db8:192:21::1/64 standby 2001:db8:192:21::2
 ipv6 enable
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.11.60 255.255.255.0 standby 192.168.11.62
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 description LAN/STATE Failover Interface
!
interface GigabitEthernet0/4
```

```
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/6
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/7
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
 nameif management
 security-level 0
 no ip address
!
banner exec WARNING:
banner exec **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
banner exec                                **** AUTHORIZED USERS ONLY! ****
banner exec
banner exec ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
banner exec TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE
NECESSARY
banner exec TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
banner exec REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME
WITHOUT
banner exec FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
banner exec CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
banner exec ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
banner exec
banner exec UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL
LAWS.
banner login WARNING:
banner login THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
banner asdm WARNING:
banner asdm   **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
banner asdm                    **** AUTHORIZED USERS ONLY! ****
banner asdm
banner asdm ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY TO
IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER REPRESENTATIVES OF THE
SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT FURTHER NOTICE OR CONSENT.
UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER CRIMINAL CONDUCT REVEALED BY SUCH USE IS
SUBJECT TO DISCLOSURE TO LAW ENFORCEMENT OFFICIALS AND PROSECUTION TO THE F
banner asdm
banner asdm UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL
LAWS
boot system disk0:/asa911-smp-k8.bin
ftp mode passive
clock timezone PST -8
clock summer-time PDT recurring
```

```
dns domain-lookup outside
dns domain-lookup inside
dns server-group DefaultDNS
 name-server 192.168.42.130
 domain-name cisco-irn.com
same-security-traffic permit inter-interface
object network PrimeLMS
 host 192.168.42.139
 description Cisco Prime LMS
object network RIE-1_G0-0-1
 host 192.168.22.11
 description ASA1002-X
object network RIE-1_G0-0-1_ipv6
 host 2001:db8:192:22::11
object network RIE-2_G0-0-2
 host 192.168.22.12
 description ASR1002-x
object network RIE-2_G0-0-2_ipv6
 host 2001:db8:192:22::12
object network RIE1+2_HSRP_ipv6
 host 2001:db8:192:22::10
object network RIE1+2_HSRP
 host 192.168.22.10
object network ASA-IE-1-outside.cisco-irn.com
 host 192.168.21.1
object network Bart-Admin99
 host 10.19.151.99
object network DMZ-Network-4
 subnet 192.168.20.24 255.255.255.248
object network DMZ-Networks
 subnet 192.168.20.0 255.255.252.0
object network DMZ-VIP-30
 host 192.168.20.30
object network DataCenter-Networks
 subnet 192.168.0.0 255.255.0.0
 description Private 1918 block
object network EMC-NCM.cisco-irn.com
 host 192.168.42.122
object network ESA-IE-1.cisco-irn.com
 host 192.168.23.68
object network ESMA-IE-1.cisco-irn.com
 host 192.168.23.84
object network EmailSecurityAppliance-Network
 subnet 192.168.23.64 255.255.255.240
object network EmailSecurityManager-Network
 subnet 192.168.23.80 255.255.255.240
object network FSU.cisco-irn.com
 host 192.168.42.138
object network InSide-Network
 subnet 192.168.21.0 255.255.255.0
object network InternetEdge-Networks
 subnet 192.168.20.0 255.255.252.0
object network NTP1.cisco-irn.com
 host 192.168.62.161
object network NTP2.cisco-irn.com
 host 192.168.62.162
object network OutSide-Network
 subnet 192.168.22.0 255.255.255.0
object network PAME-DC-1.cisco-irn.com
 host 192.168.44.111
object network RSA-enVision.cisco-irn.com
 host 192.168.42.124
object network SRV-DC-1.cisco-irn.com
 host 192.168.41.101
```

```
object network SRV-DC-2.cisco-irn.com
 host 192.168.41.102
object network Branch-Networks
 subnet 10.10.0.0 255.255.0.0
object network WebSecurityAppliance-Network
 subnet 192.168.23.96 255.255.255.240
object network csmanager.cisco-irn.com
 host 192.168.42.133
object network tacacs.cisco-irn.com
 host 192.168.42.131
object network ActiveDirectory
 host 192.168.42.130
object network LABNTP-1.cisco.com
 host 171.68.10.150
object network LABNTP-2.cisco.com
 host 171.68.10.80
object network nist-chicago-NoDNS-
 host 38.106.177.10
 description Chicago, Illinois
object network nist-time-server.eoni.com
 host 216.228.192.69
 description La Grande, Oregon
object network nist.expertsmi.com
 host 50.77.217.185
 description Monroe, Michigan
object network nist.netservicesgroup.com
 host 64.113.32.5
 description Southfield, Michigan
object network nist.time.nosc.us
 host 96.226.123.117
 description Carrollton, Texas
object network nist1-atl.ustiming.org
 host 64.250.177.145
 description Atlanta, Georgia
object network nist1-chi.ustiming.org
 host 216.171.120.36
 description Chicago, Illinois
object network nist1-la.ustiming.org
 host 64.147.116.229
 description Los Angeles, California
object network nist1-lnk.binary.net
 host 216.229.0.179
 description Lincoln, Nebraska
object network nist1-lv.ustiming.org
 host 64.250.229.100
 description Las Vegas, Nevada
object network nist1-nj.ustiming.org
 host 96.47.67.105
 description Bridgewater, NJ
object network nist1-nj2.ustiming.org
 host 165.193.126.229
 description Weehawken, NJ
object network nist1-ny.ustiming.org
 host 64.90.182.55
 description New York City, NY
object network nist1-pa.ustiming.org
 host 206.246.122.250
 description Hatfield, PA
object network nist1-sj.ustiming.org
 host 216.171.124.36
 description San Jose, California
object network nist1.aol-ca.symmetricom.com
 host 207.200.81.113
 description Mountain View, California
```

```
object network nist1.aol-va.symmetricom.com
 host 64.236.96.53
 description Reston, Virginia
object network nist1.columbiacountyga.gov
 host 216.119.63.113
 description Columbia County, Georgia
object network nist1.symmetricom.com
 host 69.25.96.13
 description San Jose, California
object network nist2-nj2.ustiming.org
 host 165.193.126.232
 description Weehawken, NJ
object network nisttime.carsoncity.k12.mi.us
 host 66.219.116.140
 description Carson City, Michigan
object network ntp-nist.ldsbc.edu
 host 198.60.73.8
 description LDSBC, Salt Lake City, Utah
object network time-a.nist.gov
 host 129.6.15.28
 description NIST, Gaithersburg, Maryland
object network time-a.timefreq.bldrdoc.gov
 host 132.163.4.101
 description NIST, Boulder, Colorado
object network time-b.nist.gov
 host 129.6.15.29
 description NIST, Gaithersburg, Maryland
object network time-b.timefreq.bldrdoc.gov
 host 132.163.4.102
 description NIST, Boulder, Colorado
object network time-c.timefreq.bldrdoc.gov
 host 132.163.4.103
 description NIST, Boulder, Colorado
object network time-d.nist.gov
 host 2610:20:6f15:15::27
 description NIST, Gaithersburg, Maryland
object network time-nw.nist.gov
 host 131.107.13.100
 description Microsoft, Redmond, Washington
object network utcnist.colorado.edu
 host 128.138.140.44
 description University of Colorado, Boulder
object network utcnist2.colorado.edu
 host 128.138.141.172
 description University of Colorado, Boulder
object network wwv.nist.gov
 host 24.56.178.140
 description WWV, Fort Collins, Colorado
object network ASA-IE-1-outside_ipv6.cisco-irn.com
 host 2001:db8:192:21::1
object network DMZ-VIP-30_ipv6
 host 2001:db8:192:20a4::30
object network CiscoLAB10-Network
 subnet 10.0.0.0 255.0.0.0
 description Private 1918 block
object network CiscoLAB171-Network
 subnet 171.68.0.0 255.255.0.0
 description ARIN Block
object network CiscoLAB172-Network
 subnet 172.16.0.0 255.240.0.0
 description Private 1918 block
object network DMZ-Network-4v6
 subnet 2001:db8:192:20a4::/64
object network EmailSecurityAppliance-Networkv6
```

```
 subnet 2001:db8:192:23a5::/64
object network EmailSecurityManager-Networkv6
 subnet 2001:db8:192:23a6::/64
object network InSide-Networkv6
 subnet 2001:db8:192:21::/64
object network OutSide-Networkv6
 subnet 2001:db8:192:22::/64
object network WebSecurityAppliance-Networkv6
 subnet 2001:db8:192:23a7::/64
object network ESA-IE-1.cisco-irn.com_ipv6
 host 2001:db8:192:23a5::68
object network ESMA-IE-1.cisco-irn.com_ipv6
 host 2001:db8:192:23a6::84
object network WSA-IE-1.cisco-irn.com
 host 192.168.23.100
object network WSA-IE-1.cisco-irn.com_ipv6
 host 2001:db8:192:23a7::100
object network ASASM-DMZ-1.cisco-irn.com
 host 192.168.21.10
object network ASASM-DMZ-2.cicso-irn.com
 host 192.168.21.12
object network ASASM-DMZ-1.cisco-irn.com_ipv6
 host 2001:db8:192:21::10
object-group service RDP tcp
 port-object eq 3389
object-group protocol TCPUDP
 protocol-object udp
 protocol-object tcp
object-group service vCenter-to-ESX4 tcp
 description Communication from vCetner to ESX hosts
 port-object eq 5989
 port-object eq 8000
 port-object eq 902
 port-object eq 903
object-group network NTP-Servers
 description NTP Servers
 network-object object NTP1.cisco-irn.com
 network-object object NTP2.cisco-irn.com
 network-object object ActiveDirectory
object-group network NTP-PublicServers
 description Public time.nist.gov servers
 network-object object nist-chicago-NoDNS-
 network-object object nist-time-server.eoni.com
 network-object object nist.expertsmi.com
 network-object object nist.netservicesgroup.com
 network-object object nist.time.nosc.us
 network-object object nist1-atl.ustiming.org
 network-object object nist1-chi.ustiming.org
 network-object object nist1-la.ustiming.org
 network-object object nist1-lnk.binary.net
 network-object object nist1-lv.ustiming.org
 network-object object nist1-nj.ustiming.org
 network-object object nist1-nj2.ustiming.org
 network-object object nist1-ny.ustiming.org
 network-object object nist1-pa.ustiming.org
 network-object object nist1-sj.ustiming.org
 network-object object nist1.aol-ca.symmetricom.com
 network-object object nist1.aol-va.symmetricom.com
 network-object object nist1.columbiacountyga.gov
 network-object object nist1.symmetricom.com
 network-object object nist2-nj2.ustiming.org
 network-object object nisttime.carsoncity.k12.mi.us
 network-object object ntp-nist.ldsbc.edu
 network-object object time-a.nist.gov
```

```
 network-object object time-a.timefreq.bldrdoc.gov
 network-object object time-b.nist.gov
 network-object object time-b.timefreq.bldrdoc.gov
 network-object object time-c.timefreq.bldrdoc.gov
 network-object object time-d.nist.gov
 network-object object time-nw.nist.gov
 network-object object utcnist.colorado.edu
 network-object object utcnist2.colorado.edu
 network-object object wwv.nist.gov
 network-object object LABNTP-1.cisco.com
 network-object object LABNTP-2.cisco.com
object-group network Admin-Systems
 network-object object PrimeLMS
 network-object object Bart-Admin99
 network-object object EMC-NCM.cisco-irn.com
 network-object object RSA-enVision.cisco-irn.com
 network-object object SRV-DC-1.cisco-irn.com
 network-object object SRV-DC-2.cisco-irn.com
 network-object object csmanager.cisco-irn.com
object-group network DM_INLINE_NETWORK_1
 network-object object EMC-NCM.cisco-irn.com
 network-object object PrimeLMS
 network-object object csmanager.cisco-irn.com
object-group network DM_INLINE_NETWORK_2
 network-object object Branch-Networks
 network-object object DataCenter-Networks
object-group network DM_INLINE_NETWORK_3
 network-object object EmailSecurityAppliance-Network
 network-object object EmailSecurityManager-Network
 network-object object WebSecurityAppliance-Network
object-group network DM_INLINE_NETWORK_4
 network-object object Branch-Networks
 network-object object DataCenter-Networks
object-group network DM_INLINE_NETWORK_5
 network-object object Branch-Networks
 network-object object DataCenter-Networks
object-group network DM_INLINE_NETWORK_6
 network-object object Branch-Networks
 network-object object DataCenter-Networks
object-group icmp-type DM_INLINE_ICMP_1
 icmp-object echo
 icmp-object echo-reply
 icmp-object information-reply
 icmp-object information-request
 icmp-object redirect
 icmp-object time-exceeded
 icmp-object traceroute
object-group service DM_INLINE_TCP_1 tcp
 group-object RDP
 port-object eq https
 port-object eq ssh
 group-object vCenter-to-ESX4
object-group service DM_INLINE_TCP_2 tcp
 port-object eq https
 port-object eq smtp
 port-object eq ssh
object-group service DM_INLINE_TCP_3 tcp
 port-object eq https
 port-object eq ssh
object-group service DM_INLINE_TCP_4 tcp
 port-object eq 1080
 port-object eq 8080
 port-object eq 8443
 port-object eq www
```

```
 port-object eq https
 port-object eq ssh
object-group network DM_INLINE_NETWORK_10
 network-object object Branch-Networks
 network-object object DataCenter-Networks
object-group network DM_INLINE_NETWORK_11
 network-object object CiscoLAB10-Network
 network-object object CiscoLAB171-Network
 network-object object CiscoLAB172-Network
object-group network DM_INLINE_NETWORK_12
 network-object object Branch-Networks
 network-object object DataCenter-Networks
object-group network DM_INLINE_NETWORK_7
 network-object object RIE-1_G0-0-1
 network-object object RIE-2_G0-0-2
 network-object object DMZ-Networks
object-group network DM_INLINE_NETWORK_8
 network-object object RIE-1_G0-0-1
 network-object object RIE-2_G0-0-2
 network-object object DMZ-Networks
 network-object object ASASM-DMZ-1.cisco-irn.com
 network-object object ASASM-DMZ-2.cicso-irn.com
object-group network DM_INLINE_NETWORK_9
 network-object object CiscoLAB10-Network
 network-object object CiscoLAB171-Network
 network-object object CiscoLAB172-Network
object-group service DM_INLINE_TCP_5 tcp
 group-object RDP
 port-object eq 1080
 port-object eq 8080
 port-object eq 8443
 port-object eq 8444
 port-object eq 8880
 port-object eq www
 port-object eq https
 port-object eq ssh
 group-object vCenter-to-ESX4
object-group network DM_INLINE_NETWORK_13
 network-object object RIE-1_G0-0-1
 network-object object RIE-2_G0-0-2
 network-object object DMZ-Networks
access-list all extended permit ip any any
access-list OUTSIDE_IN extended permit icmp6 any6 any6
access-list OUTSIDE_IN remark Clientless VPN for IPv6
access-list OUTSIDE_IN extended permit tcp any6 object ASASM-DMZ-1.cisco-irn.com_ipv6 eq
https
access-list OUTSIDE_IN remark Clientless VPN
access-list OUTSIDE_IN extended permit tcp any object ASA-IE-1-outside_ipv6.cisco-irn.com
eq https
access-list OUTSIDE_IN remark DMZ Systems send Syslog messages
access-list OUTSIDE_IN extended permit udp object-group DM_INLINE_NETWORK_7 object
RSA-enVision.cisco-irn.com eq syslog
access-list OUTSIDE_IN remark DMZ Systems Authenticate access
access-list OUTSIDE_IN extended permit tcp object-group DM_INLINE_NETWORK_8 object
tacacs.cisco-irn.com eq tacacs
access-list OUTSIDE_IN remark DMZ Systems Authenticate access
access-list OUTSIDE_IN extended permit object-group TCPUDP object-group
DM_INLINE_NETWORK_13 object ActiveDirectory eq domain
access-list OUTSIDE_IN remark ====LAB ACCESS to TEST===REMOVE===
access-list OUTSIDE_IN extended permit icmp object-group DM_INLINE_NETWORK_9 object-group
DM_INLINE_NETWORK_10
access-list OUTSIDE_IN remark ====LAB ACCESS to TEST===REMOVE===
access-list OUTSIDE_IN extended permit tcp object-group DM_INLINE_NETWORK_11 object-group
DM_INLINE_NETWORK_12 object-group DM_INLINE_TCP_5
```

```
access-list OUTSIDE_IN remark Drop all other traffic
access-list OUTSIDE_IN extended deny ip any any log
access-list DROP-ALL extended deny ip any any
access-list INSIDE_IN remark Admin Access to DMZ
access-list INSIDE_IN extended permit tcp object-group Admin-Systems object DMZ-Networks
object-group DM_INLINE_TCP_1
access-list INSIDE_IN remark Manage DMZ Devices
access-list INSIDE_IN extended permit udp object-group DM_INLINE_NETWORK_1 object
DMZ-Networks eq snmp
access-list INSIDE_IN remark Network Time
access-list INSIDE_IN extended permit udp object-group NTP-Servers object-group
NTP-PublicServers eq ntp
access-list INSIDE_IN remark Allow Access to services for Ironport Apps
access-list INSIDE_IN extended permit tcp object-group DM_INLINE_NETWORK_2 object-group
DM_INLINE_NETWORK_3 object-group DM_INLINE_TCP_2
access-list INSIDE_IN remark Allow Secure traffic to DMZ
access-list INSIDE_IN extended permit tcp object-group DM_INLINE_NETWORK_4 object
DMZ-VIP-30 object-group DM_INLINE_TCP_3
access-list INSIDE_IN remark - Block non-secure traffic to DMZ
access-list INSIDE_IN extended deny ip any object DMZ-Networks
access-list INSIDE_IN remark Allow outbound services for Internet
access-list INSIDE_IN extended permit icmp object-group DM_INLINE_NETWORK_5 any
object-group DM_INLINE_ICMP_1
access-list INSIDE_IN remark General Internet Browsing
access-list INSIDE_IN extended permit tcp object-group DM_INLINE_NETWORK_6 any
object-group DM_INLINE_TCP_4
access-list INSIDE_IN remark DNS Services
access-list INSIDE_IN extended permit object-group TCPUDP object ActiveDirectory any eq
domain
access-list INSIDE_IN remark Drop and Log all other traffic - END-OF-LINE
access-list INSIDE_IN extended deny ip any any log
access-list all-web webtype permit url any log default
pager lines 24
logging enable
logging timestamp
logging standby
logging buffer-size 1048576
logging asdm-buffer-size 512
logging trap informational
logging asdm informational
logging host inside 192.168.42.124
mtu outside 1500
mtu inside 1500
mtu management 1500
failover
failover lan unit primary
failover lan interface folink GigabitEthernet0/3
failover link folink GigabitEthernet0/3
failover interface ip folink 192.168.12.31 255.255.255.0 standby 192.168.12.32
icmp unreachable rate-limit 1 burst-size 1
icmp permit any outside
icmp permit any inside
asdm image disk0:/asdm-711.bin
asdm history enable
arp timeout 14400
no arp permit-nonconnected
access-group OUTSIDE_IN in interface outside
access-group INSIDE_IN in interface inside
access-group DROP-ALL in interface management
ipv6 icmp permit any echo outside
ipv6 icmp permit any echo-reply outside
ipv6 icmp permit any membership-query inside
ipv6 icmp permit any membership-reduction inside
ipv6 icmp permit any membership-report inside
```

```
ipv6 icmp permit any neighbor-advertisement inside
ipv6 icmp permit any neighbor-redirect inside
ipv6 icmp permit any neighbor-solicitation inside
ipv6 icmp permit any packet-too-big inside
ipv6 icmp permit any parameter-problem inside
ipv6 icmp permit any router-advertisement inside
ipv6 icmp permit any router-solicitation inside
ipv6 icmp permit any time-exceeded inside
ipv6 icmp permit any unreachable inside
ipv6 route outside ::/0 2001:db8:192:21::10
route outside 0.0.0.0 0.0.0.0 192.168.21.10 1
route inside 10.10.0.0 255.255.0.0 192.168.11.1 1
route outside 10.10.0.0 255.255.255.0 192.168.21.10 1
route inside 192.168.0.0 255.255.0.0 192.168.11.10 10
route outside 192.168.20.0 255.255.255.0 192.168.21.10 1
route outside 192.168.22.0 255.255.255.0 192.168.21.10 1
route outside 192.168.23.0 255.255.255.0 192.168.21.10 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
 network-acl all
 webvpn
  appl-acl all-web
  file-browsing enable
  file-entry enable
  http-proxy enable
  url-entry enable
  svc ask enable default webvpn
aaa-server partnerauth protocol radius
aaa-server partnerauth (inside) host 192.168.42.137
 timeout 5
 key *****
 radius-common-pw *****
aaa-server CiscoACS protocol tacacs+
 reactivation-mode depletion deadtime 15
 max-failed-attempts 5
aaa-server CiscoACS (inside) host 192.168.42.131
 key *****
user-identity default-domain LOCAL
aaa authentication enable console CiscoACS LOCAL
aaa authentication http console CiscoACS LOCAL
aaa authentication serial console CiscoACS LOCAL
aaa authentication ssh console CiscoACS LOCAL
aaa authorization command CiscoACS LOCAL
aaa accounting enable console CiscoACS
aaa accounting serial console CiscoACS
aaa accounting ssh console CiscoACS
aaa accounting command CiscoACS
aaa authentication secure-http-client
aaa local authentication attempts max-fail 6
aaa authorization exec authentication-server
http server enable
http server idle-timeout 15
http server session-timeout 15
http 192.168.41.101 255.255.255.255 inside
http 192.168.41.102 255.255.255.255 inside
http 192.168.42.122 255.255.255.255 inside
http 192.168.42.124 255.255.255.255 inside
```

```
http 192.168.42.133 255.255.255.255 inside
http 192.168.42.138 255.255.255.255 inside
http 192.168.42.139 255.255.255.255 inside
snmp-server group V3Group v3 priv
snmp-server user ciscolms V3Group v3 encrypted auth sha
56:bd:0f:20:11:a7:78:6e:08:cc:a9:43:f7:86:0e:ab:04:7c:a7:db priv aes 256
56:bd:0f:20:11:a7:78:6e:08:cc:a9:43:f7:86:0e:ab:04:7c:a7:db:88:e3:53:03:7b:f1:02:30:bc:14:
98:e5
snmp-server user csmadmin V3Group v3 encrypted auth sha
56:bd:0f:20:11:a7:78:6e:08:cc:a9:43:f7:86:0e:ab:04:7c:a7:db priv aes 256
56:bd:0f:20:11:a7:78:6e:08:cc:a9:43:f7:86:0e:ab:04:7c:a7:db:88:e3:53:03:7b:f1:02:30:bc:14:
98:e5
snmp-server host inside 192.168.42.134 version 3 ciscolms
snmp-server host inside 192.168.42.139 version 3 ciscolms
snmp-server host inside 192.168.42.133 version 3 csmadmin
snmp-server location Building SJC-17-1 Aisle 2 Rack 3
snmp-server contact EmployeeA
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
snmp-server enable traps syslog
snmp-server enable traps ipsec start stop
snmp-server enable traps memory-threshold
snmp-server enable traps interface-threshold
snmp-server enable traps remote-access session-threshold-exceeded
snmp-server enable traps connection-limit-reached
snmp-server enable traps cpu threshold rising
snmp-server enable traps ikev2 start stop
snmp-server enable traps nat packet-discard
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
ssh scopy enable
ssh 192.168.41.101 255.255.255.255 inside
ssh 192.168.41.102 255.255.255.255 inside
ssh 192.168.42.122 255.255.255.255 inside
ssh 192.168.42.124 255.255.255.255 inside
ssh 192.168.42.133 255.255.255.255 inside
ssh 192.168.42.138 255.255.255.255 inside
ssh 192.168.42.139 255.255.255.255 inside
ssh timeout 15
ssh version 2
console timeout 15
management-access inside
!
tls-proxy maximum-session 1000
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 192.168.62.162 source inside
ntp server 192.168.62.161 source inside prefer
ssl encryption 3des-sha1 aes128-sha1 aes256-sha1
webvpn
 enable outside
 anyconnect-essentials
 internal-password enable
 smart-tunnel list AllExternalApplications All-Applications * platform windows
group-policy DfltGrpPolicy attributes
 webvpn
  smart-tunnel enable AllExternalApplications
group-policy COMPLIANCE-XXX internal
group-policy COMPLIANCE-XXX attributes
 vpn-tunnel-protocol ssl-clientless
username csmadmin password 9CmOJ.jq4D54PXDW encrypted privilege 15
username ciscolms password huo2PmvTsMk6Cv1L encrypted privilege 15
```

```
username bmcgloth password gITSY3iZ3UnCQoKf encrypted privilege 15
tunnel-group DefaultRAGroup general-attributes
 authentication-server-group partnerauth
tunnel-group DefaultWEBVPNGroup general-attributes
 authentication-server-group partnerauth
tunnel-group COMPLIANCE-Lab type remote-access
tunnel-group COMPLIANCE-Lab general-attributes
 authentication-server-group partnerauth LOCAL
 default-group-policy COMPLIANCE-XXX
!
class-map inspection_default
 match default-inspection-traffic
class-map global-class-XXX
 match any
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 description IPS inspection policy for Cisco LAB
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
 class global-class-XXX
  ips inline fail-close
policy-map type inspect dns migrated_dns_map_1
 parameters
  message-length maximum client auto
  message-length maximum 512
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
password encryption aes
Cryptochecksum:d01b4c45ee6507fcc152f2f9e01983b1
: end
ASA-IE-1# $
```

DMZ-IDS-1

```
service interface
physical-interfaces GigabitEthernet0/7
subinterface-type inline-vlan-pair
subinterface 1
description INT1 vlans 83 and 84
vlan1 83
vlan2 84
exit
exit
exit
exit
! ------------------------------
service authentication
attemptLimit 6
password-strength
size 7-64
digits-min 1
lowercase-min 1
other-min 1
number-old-passwords 4
exit
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 192.168.21.93/24,192.168.21.1
host-name DMZ-IDS1
telnet-option disabled
access-list 10.19.151.99/32
access-list 192.168.41.101/32
access-list 192.168.41.102/32
access-list 192.168.42.122/32
access-list 192.168.42.124/32
access-list 192.168.42.133/32
access-list 192.168.42.138/32
dns-primary-server enabled
address 192.168.42.130
exit
dns-secondary-server disabled
dns-tertiary-server disabled
http-proxy proxy-server
address 128.107.241.169
port 80
exit
exit
time-zone-settings
offset -8
standard-time-zone-name PST
exit
ntp-option enabled-ntp-unauthenticated
ntp-server 192.168.62.161
exit
summertime-option recurring
summertime-zone-name PDT
exit
exit
! ------------------------------
service logger
```

```
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
trap-destinations 192.168.42.124
trap-community-name <removed>
exit
enable-notifications true
trap-community-name <removed>
exit
! ------------------------------
service signature-definition sig0
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
! ------------------------------
service global-correlation
exit
! ------------------------------
service aaa
aaa radius
primary-server
server-address 192.168.42.131
shared-secret <removed>
exit
nas-id DMZ-IDS1
local-fallback enabled
console-authentication radius-and-local
default-user-role administrator
exit
exit
! ------------------------------
service analysis-engine
exit
```

DMZ-ASASM

```
ASA Version 9.1(1)
!
hostname ASASM-RIE-3
domain-name cisco-irn.com
enable password <removed> encrypted
passwd <removed> encrypted
names
```

```
dns-guard
!
interface Vlan21
 nameif inside
 security-level 100
 ip address 192.168.21.10 255.255.255.0 standby 192.168.21.12
 ipv6 address 2001:db8:192:21::10/64 standby 2001:db8:192:21::12
 ipv6 enable
!
interface Vlan22
 nameif outside
 security-level 0
 ip address 192.168.22.1 255.255.255.0 standby 192.168.22.2
 ipv6 address 2001:db8:192:22::1/64 standby 2001:db8:192:22::3
 ipv6 enable
!
interface Vlan82
 nameif DMZ
 security-level 20
 ip address 192.168.20.25 255.255.255.248 standby 192.168.20.26
 ipv6 address 2001:db8:192:20a4::25/64 standby 2001:db8:192:20a4::26
 ipv6 enable
!
interface Vlan91
 description LAN Failover Interface
!
interface Vlan92
 description STATE Failover Interface
!
interface Vlan2305
 nameif EmailSecurityAppliance
 security-level 50
 ip address 192.168.23.65 255.255.255.240 standby 192.168.23.66
 ipv6 address 2001:db8:192:23a5::65/64 standby 2001:db8:192:23a5::66
 ipv6 enable
!
interface Vlan2306
 nameif EmailSecurityMgrAppliance
 security-level 60
 ip address 192.168.23.81 255.255.255.240 standby 192.168.23.82
 ipv6 address 2001:db8:192:23a6::81/64 standby 2001:db8:192:23a6::82
 ipv6 enable
!
interface Vlan2307
 shutdown
 nameif WebSecurityAppliance
 security-level 40
 ip address 192.168.23.97 255.255.255.240 standby 192.168.23.98
 ipv6 address 2001:db8:192:23a7::97/64 standby 2001:db8:192:23a7::98
 ipv6 enable
!
banner exec WARNING:
banner exec     **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
banner exec                      **** AUTHORIZED USERS ONLY! ****
banner exec
banner exec ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
banner exec TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE
NECESSARY
banner exec TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
banner exec REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME
WITHOUT
banner exec FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
banner exec CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
banner exec ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
```

```
banner exec
banner exec UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL
LAWS.
banner login WARNING:
banner login THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
banner asdm WARNING:
banner asdm     **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
banner asdm                      **** AUTHORIZED USERS ONLY! ****
banner asdm
banner asdm ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
banner asdm TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE
NECESSARY
banner asdm TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
banner asdm REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME
WITHOUT
banner asdm FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
banner asdm CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
banner asdm ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
banner asdm
banner asdm UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL
LAWS
boot system disk0:/asa911-smp-k8.bin
boot system disk0:/asa901-smp-k8.bin
ftp mode passive
dns domain-lookup inside
dns server-group DefaultDNS
 name-server 192.168.42.130
 domain-name cisco-irn.com
same-security-traffic permit inter-interface
object network PrimeLMS
 host 192.168.42.139
 description Cisco Prime LMS
object network RIE-1_G0-0-1
 host 192.168.22.11
 description ASA1002-X
object network RIE-1_G0-0-1_ipv6
 host 2001:db8:192:22::11
object network RIE-2_G0-0-2
 host 192.168.22.12
 description ASR1002-x
object network RIE-2_G0-0-2_ipv6
 host 2001:db8:192:22::12
object network RIE1+2_HSRP_ipv6
 host 2001:db8:192:22::10
object network RIE1+2_HSRP
 host 192.168.22.10
object network ASA-IE-1-outside.cisco-irn.com
 host 192.168.21.1
object network Bart-Admin99
 host 10.19.151.99
object network DMZ-Network-4
 subnet 192.168.20.24 255.255.255.248
object network DMZ-Networks
 subnet 192.168.20.0 255.255.255.0
object network DMZ-VIP-30
 host 192.168.20.30
object network DataCenter-Networks
 subnet 192.168.0.0 255.255.0.0
 description Private 1918 block
object network EMC-NCM.cisco-irn.com
 host 192.168.42.122
object network ESA-IE-1.cisco-irn.com
 host 192.168.23.68
object network ESMA-IE-1.cisco-irn.com
```

```
 host 192.168.23.84
object network EmailSecurityAppliance-Network
 subnet 192.168.23.64 255.255.255.240
object network EmailSecurityManager-Network
 subnet 192.168.23.80 255.255.255.240
object network FSU.cisco-irn.com
 host 192.168.42.138
object network InSide-Network
 subnet 192.168.21.0 255.255.255.0
object network InternetEdge-Networks
 subnet 192.168.20.0 255.255.252.0
object network NTP1.cisco-irn.com
 host 192.168.62.161
object network NTP2.cisco-irn.com
 host 192.168.62.162
object network OutSide-Network
 subnet 192.168.22.0 255.255.255.0
object network PAME-DC-1.cisco-irn.com
 host 192.168.44.111
object network RSA-enVision.cisco-irn.com
 host 192.168.42.124
object network SRV-DC-1.cisco-irn.com
 host 192.168.41.101
object network SRV-DC-2.cisco-irn.com
 host 192.168.41.102
object network Branch-Networks
 subnet 10.10.0.0 255.255.0.0
object network WebSecurityAppliance-Network
 subnet 192.168.23.96 255.255.255.240
object network csmanager.cisco-irn.com
 host 192.168.42.133
object network tacacs.cisco-irn.com
 host 192.168.42.131
object network ActiveDirectory
 host 192.168.42.130
object network LABNTP-1.cisco.com
 host 172.26.129.252
object network LABNTP-2.cisco.com
 host 172.28.189.1
object network nist-chicago-NoDNS-
 host 38.106.177.10
 description Chicago, Illinois
object network nist-time-server.eoni.com
 host 216.228.192.69
 description La Grande, Oregon
object network nist.expertsmi.com
 host 50.77.217.185
 description Monroe, Michigan
object network nist.netservicesgroup.com
 host 64.113.32.5
 description Southfield, Michigan
object network nist.time.nosc.us
 host 96.226.123.117
 description Carrollton, Texas
object network nist1-atl.ustiming.org
 host 64.250.177.145
 description Atlanta, Georgia
object network nist1-chi.ustiming.org
 host 216.171.120.36
 description Chicago, Illinois
object network nist1-la.ustiming.org
 host 64.147.116.229
 description Los Angeles, California
object network nist1-lnk.binary.net
```

```
 host 216.229.0.179
 description Lincoln, Nebraska
object network nist1-lv.ustiming.org
 host 64.250.229.100
 description Las Vegas, Nevada
object network nist1-nj.ustiming.org
 host 96.47.67.105
 description Bridgewater, NJ
object network nist1-nj2.ustiming.org
 host 165.193.126.229
 description Weehawken, NJ
object network nist1-ny.ustiming.org
 host 64.90.182.55
 description New York City, NY
object network nist1-pa.ustiming.org
 host 206.246.122.250
 description Hatfield, PA
object network nist1-sj.ustiming.org
 host 216.171.124.36
 description San Jose, California
object network nist1.aol-ca.symmetricom.com
 host 207.200.81.113
 description Mountain View, California
object network nist1.aol-va.symmetricom.com
 host 64.236.96.53
 description Reston, Virginia
object network nist1.columbiacountyga.gov
 host 216.119.63.113
 description Columbia County, Georgia
object network nist1.symmetricom.com
 host 69.25.96.13
 description San Jose, California
object network nist2-nj2.ustiming.org
 host 165.193.126.232
 description Weehawken, NJ
object network nisttime.carsoncity.k12.mi.us
 host 66.219.116.140
 description Carson City, Michigan
object network ntp-nist.ldsbc.edu
 host 198.60.73.8
 description LDSBC, Salt Lake City, Utah
object network time-a.nist.gov
 host 129.6.15.28
 description NIST, Gaithersburg, Maryland
object network time-a.timefreq.bldrdoc.gov
 host 132.163.4.101
 description NIST, Boulder, Colorado
object network time-b.nist.gov
 host 129.6.15.29
 description NIST, Gaithersburg, Maryland
object network time-b.timefreq.bldrdoc.gov
 host 132.163.4.102
 description NIST, Boulder, Colorado
object network time-c.timefreq.bldrdoc.gov
 host 132.163.4.103
 description NIST, Boulder, Colorado
object network time-d.nist.gov
 host 2610:20:6f15:15::27
 description NIST, Gaithersburg, Maryland
object network time-nw.nist.gov
 host 131.107.13.100
 description Microsoft, Redmond, Washington
object network utcnist.colorado.edu
 host 128.138.140.44
```

```
 description University of Colorado, Boulder
object network utcnist2.colorado.edu
 host 128.138.141.172
 description University of Colorado, Boulder
object network wwv.nist.gov
 host 24.56.178.140
 description WWV, Fort Collins, Colorado
object network ASA-IE-1-outside_ipv6.cisco-irn.com
 host 2001:db8:192:21::1
object network DMZ-VIP-30_ipv6
 host 2001:db8:192:20a4::30
object network CiscoLAB10-Network
 subnet 10.0.0.0 255.0.0.0
 description Private 1918 block
object network CiscoLAB171-Network
 subnet 171.68.0.0 255.255.0.0
 description ARIN Block
object network CiscoLAB172-Network
 subnet 172.16.0.0 255.240.0.0
 description Private 1918 block
object network DMZ-Network-4v6
 subnet 2001:db8:192:20a4::/64
object network EmailSecurityAppliance-Networkv6
 subnet 2001:db8:192:23a5::/64
object network EmailSecurityManager-Networkv6
 subnet 2001:db8:192:23a6::/64
object network InSide-Networkv6
 subnet 2001:db8:192:21::/64
object network OutSide-Networkv6
 subnet 2001:db8:192:22::/64
object network WebSecurityAppliance-Networkv6
 subnet 2001:db8:192:23a7::/64
object network ESA-IE-1.cisco-irn.com_ipv6
 host 2001:db8:192:23a5::68
object network ESMA-IE-1.cisco-irn.com_ipv6
 host 2001:db8:192:23a6::84
object network WSA-IE-1.cisco-irn.com
 host 192.168.23.100
object network WSA-IE-1.cisco-irn.com_ipv6
 host 2001:db8:192:23a7::100
object-group icmp-type DM_INLINE_ICMP_1
 icmp-object echo
 icmp-object echo-reply
 icmp-object information-reply
 icmp-object redirect
 icmp-object time-exceeded
 icmp-object traceroute
object-group network DM_INLINE_NETWORK_27
 network-object object ESA-IE-1.cisco-irn.com
 network-object object ESA-IE-1.cisco-irn.com_ipv6
object-group protocol ICMP-v6
 protocol-object icmp6
object-group network DM_INLINE_NETWORK_20
 network-object object ESA-IE-1.cisco-irn.com
 network-object object ESA-IE-1.cisco-irn.com_ipv6
object-group service DM_INLINE_SERVICE_1
 service-object tcp destination eq https
 service-object tcp destination eq ssh
object-group network NTP-Servers
 description NTP Servers
 network-object object NTP1.cisco-irn.com
 network-object object NTP2.cisco-irn.com
 network-object object ActiveDirectory
object-group network DM_INLINE_NETWORK_6
```

```
 network-object object EmailSecurityAppliance-Network
 network-object object EmailSecurityManager-Network
 network-object object WebSecurityAppliance-Network
object-group service RDP tcp
 port-object eq 3389
object-group service vCenter-to-ESX4 tcp
 description Communication from vCetner to ESX hosts
 port-object eq 5989
 port-object eq 8000
 port-object eq 902
 port-object eq 903
object-group service DM_INLINE_TCP_2 tcp
 group-object RDP
 port-object eq https
 port-object eq ssh
 group-object vCenter-to-ESX4
object-group service DM_INLINE_UDP_1 udp
 port-object eq 1812
 port-object eq 1813
object-group service DM_INLINE_UDP_2 udp
 port-object eq 1812
 port-object eq 1813
object-group network DM_INLINE_NETWORK_2
 network-object object EMC-NCM.cisco-irn.com
 network-object object PrimeLMS
 network-object object csmanager.cisco-irn.com
object-group service DM_INLINE_UDP_3 udp
 port-object eq 1812
 port-object eq 1813
object-group network DM_INLINE_NETWORK_21
 network-object object Branch-Networks
 network-object object DataCenter-Networks
object-group service DM_INLINE_TCP_3 tcp
 port-object eq https
 port-object eq smtp
 port-object eq ssh
object-group network DM_INLINE_NETWORK_22
 network-object object Branch-Networks
 network-object object DataCenter-Networks
object-group network DM_INLINE_NETWORK_23
 network-object object Branch-Networks
 network-object object DataCenter-Networks
object-group network Admin-Systems
 network-object object PrimeLMS
 network-object object Bart-Admin99
 network-object object EMC-NCM.cisco-irn.com
 network-object object RSA-enVision.cisco-irn.com
 network-object object SRV-DC-1.cisco-irn.com
 network-object object SRV-DC-2.cisco-irn.com
 network-object object csmanager.cisco-irn.com
object-group network DM_INLINE_NETWORK_24
 network-object object Branch-Networks
 network-object object DataCenter-Networks
object-group service DM_INLINE_TCP_4 tcp
 port-object eq https
 port-object eq ssh
object-group service DM_INLINE_TCP_5 tcp
 port-object eq 1080
 port-object eq 8080
 port-object eq 8443
 port-object eq www
 port-object eq https
 port-object eq ssh
object-group network DM_INLINE_NETWORK_25
```

```
 network-object object RIE-1_G0-0-1
 network-object object RIE-2_G0-0-2
object-group network DM_INLINE_NETWORK_26
 network-object object RIE-1_G0-0-1
 network-object object RIE-2_G0-0-2
object-group network DM_INLINE_NETWORK_3
 network-object object DataCenter-Networks
 network-object object Branch-Networks
object-group network NTP-PublicServers
 description Public time.nist.gov servers
 network-object object LABNTP-1.cisco.com
 network-object object LABNTP-2.cisco.com
 network-object object nist-chicago-NoDNS-
 network-object object nist-time-server.eoni.com
 network-object object nist.expertsmi.com
 network-object object nist.netservicesgroup.com
 network-object object nist.time.nosc.us
 network-object object nist1-atl.ustiming.org
 network-object object nist1-chi.ustiming.org
 network-object object nist1-la.ustiming.org
 network-object object nist1-lnk.binary.net
 network-object object nist1-lv.ustiming.org
 network-object object nist1-nj.ustiming.org
 network-object object nist1-nj2.ustiming.org
 network-object object nist1-ny.ustiming.org
 network-object object nist1-pa.ustiming.org
 network-object object nist1-sj.ustiming.org
 network-object object nist1.aol-ca.symmetricom.com
 network-object object nist1.aol-va.symmetricom.com
 network-object object nist1.columbiacountyga.gov
 network-object object nist1.symmetricom.com
 network-object object nist2-nj2.ustiming.org
 network-object object nisttime.carsoncity.k12.mi.us
 network-object object ntp-nist.ldsbc.edu
 network-object object time-a.nist.gov
 network-object object time-a.timefreq.bldrdoc.gov
 network-object object time-b.nist.gov
 network-object object time-b.timefreq.bldrdoc.gov
 network-object object time-c.timefreq.bldrdoc.gov
 network-object object time-d.nist.gov
 network-object object time-nw.nist.gov
 network-object object utcnist.colorado.edu
 network-object object utcnist2.colorado.edu
 network-object object wwv.nist.gov
object-group network DM_INLINE_NETWORK_4
 network-object object DMZ-VIP-30
 network-object object DMZ-VIP-30_ipv6
object-group network DM_INLINE_NETWORK_5
 network-object object ASA-IE-1-outside.cisco-irn.com
 network-object object ASA-IE-1-outside_ipv6.cisco-irn.com
object-group network DM_INLINE_NETWORK_7
 network-object object DataCenter-Networks
 network-object object Branch-Networks
object-group service DM_INLINE_TCP_1 tcp
 group-object RDP
 port-object eq www
 port-object eq https
 port-object eq ssh
 group-object vCenter-to-ESX4
 port-object eq 1080
 port-object eq 8080
 port-object eq 8443
 port-object eq 8444
 port-object eq 8880
```

```
object-group network DM_INLINE_NETWORK_8
 network-object object CiscoLAB10-Network
 network-object object CiscoLAB171-Network
 network-object object CiscoLAB172-Network
object-group network DM_INLINE_NETWORK_9
 network-object object CiscoLAB10-Network
 network-object object CiscoLAB171-Network
 network-object object CiscoLAB172-Network
object-group network DM_INLINE_NETWORK_1
 network-object object WSA-IE-1.cisco-irn.com
 network-object object WSA-IE-1.cisco-irn.com_ipv6
object-group network DM_INLINE_NETWORK_10
 network-object object ESMA-IE-1.cisco-irn.com
 network-object object ESMA-IE-1.cisco-irn.com_ipv6
object-group network DM_INLINE_NETWORK_11
 network-object object WSA-IE-1.cisco-irn.com
 network-object object WSA-IE-1.cisco-irn.com_ipv6
object-group network DM_INLINE_NETWORK_12
 network-object object ESMA-IE-1.cisco-irn.com
 network-object object ESMA-IE-1.cisco-irn.com_ipv6
object-group network DM_INLINE_NETWORK_13
 network-object object ESA-IE-1.cisco-irn.com
 network-object object ESA-IE-1.cisco-irn.com_ipv6
object-group network DM_INLINE_NETWORK_14
 network-object object WebSecurityAppliance-Network
 network-object object WebSecurityAppliance-Networkv6
object-group network DM_INLINE_NETWORK_15
 network-object object DataCenter-Networks
 network-object object Branch-Networks
object-group network DM_INLINE_NETWORK_16
 network-object object EmailSecurityManager-Network
 network-object object EmailSecurityManager-Networkv6
object-group network DM_INLINE_NETWORK_17
 network-object object DataCenter-Networks
 network-object object Branch-Networks
object-group network DM_INLINE_NETWORK_18
 network-object object EmailSecurityAppliance-Network
 network-object object EmailSecurityAppliance-Networkv6
object-group network DM_INLINE_NETWORK_19
 network-object object DataCenter-Networks
 network-object object Branch-Networks
object-group service DM_INLINE_SERVICE_2
 service-object tcp-udp destination eq domain
 service-object tcp destination eq smtp
object-group service DM_INLINE_SERVICE_3
 service-object tcp-udp destination eq domain
 service-object tcp destination eq www
 service-object tcp destination eq https
object-group service DM_INLINE_SERVICE_4
 service-object tcp-udp destination eq domain
 service-object tcp destination eq smtp
object-group service DM_INLINE_SERVICE_5
 service-object tcp-udp destination eq domain
 service-object tcp destination eq www
 service-object tcp destination eq https
object-group service DM_INLINE_SERVICE_6
 service-object tcp-udp destination eq domain
 service-object tcp destination eq smtp
object-group service DM_INLINE_SERVICE_7
 service-object tcp-udp destination eq domain
 service-object tcp destination eq smtp
object-group protocol TCPUDP
 protocol-object udp
 protocol-object tcp
```

```
access-list Ironport-ESA_IN remark IPv6 Discovery-opperation
access-list Ironport-ESA_IN extended permit object-group ICMP-v6 any6 any6
access-list Ironport-ESA_IN remark Block traffic from DMZ to Internal networks
access-list Ironport-ESA_IN extended deny object-group DM_INLINE_SERVICE_7 object-group
DM_INLINE_NETWORK_18 object-group DM_INLINE_NETWORK_19
access-list Ironport-ESA_IN remark DNS lookup and Mail to Internet
access-list Ironport-ESA_IN extended permit object-group DM_INLINE_SERVICE_4 object-group
DM_INLINE_NETWORK_27 any
access-list Ironport-ESA_IN remark Network Time
access-list Ironport-ESA_IN extended permit udp object-group DM_INLINE_NETWORK_13
object-group NTP-PublicServers eq ntp
access-list Ironport-ESA_IN remark Logging
access-list Ironport-ESA_IN extended permit udp object ESA-IE-1.cisco-irn.com object
RSA-enVision.cisco-irn.com eq syslog
access-list Ironport-ESA_IN remark Authentication
access-list Ironport-ESA_IN extended permit udp object ESA-IE-1.cisco-irn.com object
tacacs.cisco-irn.com object-group DM_INLINE_UDP_1
access-list DMZ-WebServers_IN remark IPv6 Discovery-opperation
access-list DMZ-WebServers_IN extended permit object-group ICMP-v6 any6 any6
access-list DMZ-WebServers_IN remark Logging
access-list DMZ-WebServers_IN extended permit udp object DMZ-Networks object
RSA-enVision.cisco-irn.com eq syslog
access-list DMZ-WebServers_IN remark Authentication
access-list DMZ-WebServers_IN extended permit tcp object DMZ-Networks object
tacacs.cisco-irn.com eq tacacs
access-list DMZ-WebServers_IN remark Network Time
access-list DMZ-WebServers_IN extended permit udp object DMZ-Networks object-group
NTP-PublicServers eq ntp
access-list Ironport-ESMA_IN remark IPv6 Discovery-opperation
access-list Ironport-ESMA_IN extended permit object-group ICMP-v6 any6 any6
access-list Ironport-ESMA_IN remark Block traffic from DMZ to Internal networks
access-list Ironport-ESMA_IN extended deny object-group DM_INLINE_SERVICE_6 object-group
DM_INLINE_NETWORK_16 object-group DM_INLINE_NETWORK_17
access-list Ironport-ESMA_IN remark DNS Lookup and Mail relay
access-list Ironport-ESMA_IN extended permit object-group DM_INLINE_SERVICE_2 object-group
DM_INLINE_NETWORK_10 any
access-list Ironport-ESMA_IN remark Network Time
access-list Ironport-ESMA_IN extended permit udp object-group DM_INLINE_NETWORK_12
object-group NTP-PublicServers eq ntp
access-list Ironport-ESMA_IN remark Logging
access-list Ironport-ESMA_IN extended permit udp object ESMA-IE-1.cisco-irn.com object
RSA-enVision.cisco-irn.com eq syslog
access-list Ironport-ESMA_IN remark Authentication
access-list Ironport-ESMA_IN extended permit udp object ESMA-IE-1.cisco-irn.com object
tacacs.cisco-irn.com object-group DM_INLINE_UDP_2
access-list INSIDE remark Admin Access to DMZ
access-list INSIDE extended permit tcp object-group Admin-Systems object
InternetEdge-Networks object-group DM_INLINE_TCP_2
access-list INSIDE remark Manage DMZ Devices
access-list INSIDE extended permit udp object-group DM_INLINE_NETWORK_2 object
InternetEdge-Networks eq snmp
access-list INSIDE remark Network Time
access-list INSIDE extended permit udp object-group NTP-Servers object-group
NTP-PublicServers eq ntp
access-list INSIDE remark Allow Access to services for Ironport Apps
access-list INSIDE extended permit tcp object-group DM_INLINE_NETWORK_22 object-group
DM_INLINE_NETWORK_6 object-group DM_INLINE_TCP_3
access-list INSIDE remark Allow Secure traffic to DMZ
access-list INSIDE extended permit tcp object-group DM_INLINE_NETWORK_21 object DMZ-VIP-30
object-group DM_INLINE_TCP_4
access-list INSIDE remark - Block non-secure traffic to DMZ
access-list INSIDE extended deny ip any object InternetEdge-Networks log
access-list INSIDE remark Allow outbound services for Internet
```

```
access-list INSIDE extended permit icmp object-group DM_INLINE_NETWORK_23 any object-group
DM_INLINE_ICMP_1
access-list INSIDE remark General Internet Browsing
access-list INSIDE extended permit tcp object-group DM_INLINE_NETWORK_24 any object-group
DM_INLINE_TCP_5
access-list INSIDE remark DNS Services
access-list INSIDE extended permit object-group TCPUDP object ActiveDirectory any eq
domain
access-list INSIDE remark Drop and Log all other traffic - END-OF-LINE
access-list INSIDE extended deny ip any any log
access-list OUTSIDE remark IPv6 Discovery-opperation
access-list OUTSIDE extended permit object-group ICMP-v6 any6 any6
access-list OUTSIDE remark Allow traffic to DMZ e-commerce Server
access-list OUTSIDE extended permit object-group DM_INLINE_SERVICE_1 any object-group
DM_INLINE_NETWORK_4
access-list OUTSIDE remark Mail to Ironport
access-list OUTSIDE extended permit tcp any object-group DM_INLINE_NETWORK_20 eq smtp
access-list OUTSIDE remark Remote Access SSL VPN
access-list OUTSIDE extended permit tcp any object-group DM_INLINE_NETWORK_5 eq https
access-list OUTSIDE remark Allow traffic from edge routers - RIE-1
access-list OUTSIDE extended permit udp object-group DM_INLINE_NETWORK_25 object
RSA-enVision.cisco-irn.com eq syslog
access-list OUTSIDE remark Allow traffic from edge routers - RIE-1
access-list OUTSIDE extended permit tcp object-group DM_INLINE_NETWORK_26 object
tacacs.cisco-irn.com eq tacacs
access-list OUTSIDE remark ====LAB ACCESS to TEST===REMOVE===
access-list OUTSIDE extended permit icmp object-group DM_INLINE_NETWORK_9 object-group
DM_INLINE_NETWORK_7
access-list OUTSIDE remark ====LAB ACCESS TO TEST===REMOVE====
access-list OUTSIDE extended permit tcp object-group DM_INLINE_NETWORK_8 object-group
DM_INLINE_NETWORK_3 object-group DM_INLINE_TCP_1
access-list OUTSIDE remark Drop all other traffic
access-list OUTSIDE extended deny ip any any log
access-list Ironport-WSA_IN remark IPv6 Discovery-opperation
access-list Ironport-WSA_IN extended permit object-group ICMP-v6 any6 any6
access-list Ironport-WSA_IN remark Block traffic from DMZ to Internal networks
access-list Ironport-WSA_IN extended deny object-group DM_INLINE_SERVICE_5 object-group
DM_INLINE_NETWORK_14 object-group DM_INLINE_NETWORK_15
access-list Ironport-WSA_IN remark DNS Lookup, Web Surfing
access-list Ironport-WSA_IN extended permit object-group DM_INLINE_SERVICE_3 object-group
DM_INLINE_NETWORK_11 any
access-list Ironport-WSA_IN remark Network Time
access-list Ironport-WSA_IN extended permit udp object-group DM_INLINE_NETWORK_1
object-group NTP-PublicServers eq ntp
access-list Ironport-WSA_IN remark Logging
access-list Ironport-WSA_IN extended permit udp object WSA-IE-1.cisco-irn.com object
RSA-enVision.cisco-irn.com eq syslog
access-list Ironport-WSA_IN remark Authentication
access-list Ironport-WSA_IN extended permit udp object WSA-IE-1.cisco-irn.com object
tacacs.cisco-irn.com object-group DM_INLINE_UDP_3
pager lines 24
logging enable
logging standby
logging buffer-size 1048576
logging asdm-buffer-size 512
logging asdm informational
logging host inside 192.168.42.124
mtu inside 1500
mtu outside 1500
mtu DMZ 1500
mtu EmailSecurityAppliance 1500
mtu EmailSecurityMgrAppliance 1500
mtu WebSecurityAppliance 1500
failover
```

```
failover lan unit primary
failover lan interface failover Vlan91
failover link statelink Vlan92
failover interface ip failover 192.168.20.13 255.255.255.252 standby 192.168.20.14
failover interface ip statelink 192.168.20.33 255.255.255.252 standby 192.168.20.34
icmp unreachable rate-limit 1 burst-size 1
icmp permit any inside
icmp permit any outside
icmp permit any DMZ
icmp permit any EmailSecurityAppliance
icmp permit any EmailSecurityMgrAppliance
icmp permit any WebSecurityAppliance
asdm image disk0:/asdm-711.bin
asdm history enable
arp timeout 14400
no arp permit-nonconnected
access-group INSIDE in interface inside
access-group OUTSIDE in interface outside
access-group DMZ-WebServers_IN in interface DMZ
access-group Ironport-ESA_IN in interface EmailSecurityAppliance
access-group Ironport-ESMA_IN in interface EmailSecurityMgrAppliance
access-group Ironport-WSA_IN in interface WebSecurityAppliance
ipv6 route DMZ 2001:db8:192:20a1::/64 2001:db8:192:20a4::28
ipv6 route outside ::/0 2001:db8:192:22::10
route outside 0.0.0.0 0.0.0.0 192.168.22.10 1
route inside 10.10.0.0 255.255.0.0 192.168.21.1 1
route outside 10.10.0.0 255.255.255.0 192.168.22.10 1
route outside 10.10.3.0 255.255.255.0 192.168.22.11 1
route outside 10.10.4.0 255.255.255.0 192.168.22.12 1
route inside 192.168.0.0 255.255.0.0 192.168.21.1 1
route DMZ 192.168.20.0 255.255.255.248 192.168.20.28 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
aaa-server CiscoACS protocol tacacs+
 reactivation-mode depletion deadtime 15
 max-failed-attempts 5
aaa-server CiscoACS (inside) host 192.168.42.131
 key *****
user-identity default-domain LOCAL
aaa authentication enable console CiscoACS LOCAL
aaa authentication http console CiscoACS LOCAL
aaa authentication ssh console CiscoACS LOCAL
aaa authentication serial console CiscoACS LOCAL
aaa authorization command CiscoACS LOCAL
aaa accounting enable console CiscoACS
aaa accounting serial console CiscoACS
aaa accounting ssh console CiscoACS
aaa accounting command privilege 15 CiscoACS
aaa authentication secure-http-client
aaa local authentication attempts max-fail 6
aaa authorization exec authentication-server
http server enable
http server idle-timeout 15
http server session-timeout 15
http 192.168.41.101 255.255.255.255 inside
http 192.168.41.102 255.255.255.255 inside
http 192.168.42.122 255.255.255.255 inside
```

```
http 192.168.42.124 255.255.255.255 inside
http 192.168.42.133 255.255.255.255 inside
http 192.168.42.138 255.255.255.255 inside
http 192.168.42.139 255.255.255.255 inside
snmp-server group Authentication&Encryption v3 priv
snmp-server user ciscolms Authentication&Encryption v3 encrypted auth sha
22:c2:d0:4d:34:22:54:cd:e7:15:55:63:70:0e:b9:49:c6:09:75:17 priv aes 256
22:c2:d0:4d:34:22:54:cd:e7:15:55:63:70:0e:b9:49:c6:09:75:17:14:95:f7:2f:f8:6a:ee:62:d6:03:
7f:db
snmp-server user csmadmin Authentication&Encryption v3 encrypted auth sha
22:c2:d0:4d:34:22:54:cd:e7:15:55:63:70:0e:b9:49:c6:09:75:17 priv aes 256
22:c2:d0:4d:34:22:54:cd:e7:15:55:63:70:0e:b9:49:c6:09:75:17:14:95:f7:2f:f8:6a:ee:62:d6:03:
7f:db
snmp-server host inside 192.168.42.134 version 3 ciscolms
snmp-server host inside 192.168.42.139 version 3 ciscolms
snmp-server host inside 192.168.42.133 version 3 csmadmin
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
no snmp-server enable
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
ssh scopy enable
ssh 192.168.41.101 255.255.255.255 inside
ssh 192.168.41.102 255.255.255.255 inside
ssh 192.168.42.122 255.255.255.255 inside
ssh 192.168.42.124 255.255.255.255 inside
ssh 192.168.42.133 255.255.255.255 inside
ssh 192.168.42.138 255.255.255.255 inside
ssh 192.168.42.139 255.255.255.255 inside
ssh timeout 15
ssh version 2
console timeout 15
!
tls-proxy maximum-session 1000
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ssl encryption aes256-sha1 aes128-sha1 3des-sha1
username csmadmin password 9CmOJ.jq4D54PXDW encrypted privilege 15
username bmcgloth password gITSY3iZ3UnCQoKf encrypted privilege 15
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect skinny
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
```

```
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly 8
  subscribe-to-alert-group configuration periodic monthly 8
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:3461835c1b952f647c39ea90dc41d8b4
: end
```

DMZ-ACE-1

```
logging enable
logging timestamp
logging trap 6
logging buffered 6
logging device-id context-name
logging host 192.168.42.124 udp/514
logging rate-limit 1 120 message 302027

login timeout 15
hostname ACE1
boot system image:c6ace-t1k9-mz.A5_1_2.bin

resource-class Gold
  limit-resource all minimum 0.00 maximum unlimited
  limit-resource conc-connections minimum 10.00 maximum unlimited
  limit-resource sticky minimum 10.00 maximum unlimited
tacacs-server host 192.168.42.131 key 7 <removed>
aaa group server tacacs+ CiscoACS
  server 192.168.42.131

clock timezone standard PST
clock summer-time standard PDT
aaa authentication login default group CiscoACS local
aaa authentication login console group CiscoACS local
aaa accounting default group CiscoACS local



class-map type management match-any remote-mgmt
  9 match protocol ssh source-address 192.168.41.102 255.255.255.255
  10 match protocol ssh source-address 192.168.42.131 255.255.255.255
  30 match protocol icmp any
  32 match protocol ssh source-address 192.168.41.101 255.255.255.255
  33 match protocol ssh source-address 192.168.42.111 255.255.255.255
  34 match protocol ssh source-address 192.168.42.122 255.255.255.255
  35 match protocol ssh source-address 192.168.42.124 255.255.255.255
  36 match protocol ssh source-address 192.168.42.133 255.255.255.255
  37 match protocol ssh source-address 192.168.42.138 255.255.255.255

policy-map type management first-match remote-access
  class remote-mgmt
    permit

interface vlan 21
  ip address 192.168.21.95 255.255.255.0
```

```
  service-policy input remote-access
  no shutdown

ft interface vlan 85
  ip address 192.168.20.9 255.255.255.252
  peer ip address 192.168.20.10 255.255.255.252
  no shutdown

ft peer 1
  heartbeat interval 300
  heartbeat count 10
  ft-interface vlan 85
ft group 11
  peer 1
  priority 110
  peer priority 105
  associate-context Admin
  inservice

domain cisco-irn.com

ip route 0.0.0.0 0.0.0.0 192.168.21.1

context ECOM
  allocate-interface vlan 82-83
  allocate-interface vlan 95



ft group 10
  peer 1
  priority 110
  peer priority 105
  associate-context ECOM
  inservice
username csmadmin password 5 <removed>  role Admin domain default-domain cisco-irn.com
username bmcgloth password 5 <removed>  role Admin domain default-domain cisco-irn.com
username lmsadmin password 5 <removed>  role Admin domain default-domain cisco-irn.com

ssh key rsa 2048 force
```

DMZ-ACE-1_ECOM

```
logging enable
logging timestamp
logging buffered 7
logging monitor 7
logging device-id context-name
logging host 192.168.42.124 udp/514
logging rate-limit 1 120 message 302027



login timeout 15
tacacs-server host 192.168.42.131 key 7 <removed>
aaa group server tacacs+ CiscoACS
  server 192.168.42.131
aaa authentication login default group CiscoACS local
aaa authentication login console group CiscoACS local
aaa accounting default group CiscoACS local
```

```
access-list in2out line 10 extended permit ip host 192.168.20.2 any
access-list in2out line 12 extended permit ip host 192.168.20.1 any
access-list in2out line 15 extended deny ip any any
access-list out2in line 10 extended permit tcp any host 192.168.20.1 eq ssh
access-list out2in line 11 extended permit tcp any host 192.168.20.2 eq ssh
access-list out2in line 12 extended permit tcp any host 192.168.20.1 eq https
access-list out2in line 13 extended permit tcp any host 192.168.20.2 eq https
access-list out2in line 14 extended permit icmp any host 192.168.20.1
access-list out2in line 15 extended permit icmp any host 192.168.20.2
access-list out2in line 16 extended deny ip any any
access-list out2in_ipv6 line 8 extended permit icmpv6 anyv6 host 2001:db8:192:20a1::1
access-list out2in_ipv6 line 16 extended permit tcp anyv6 host 2001:db8:192:20a1::1 eq ssh
access-list out2in_ipv6 line 24 extended permit tcp anyv6 host 2001:db8:192:20a1::1 eq
https


probe icmp ICMP
  interval 2
  faildetect 2
  passdetect count 2


rserver host ECOM
  ip address 192.168.20.2
  inservice

serverfarm host LAB-ECOM
  predictor leastconns
  probe ICMP
  rserver ECOM
    inservice

class-map match-any ECOMVIP
  5 match virtual-address 2001:db8:192:20a1::1 tcp eq 22
  6 match virtual-address 2001:db8:192:20a1::1 tcp eq https
class-map match-any ECOMVIP_v4
  3 match virtual-address 192.168.20.1 tcp eq 22
  4 match virtual-address 192.168.20.1 tcp eq https
class-map type management match-any MANAGEMENT
  7 match protocol icmp any
  8 match protocol ssh source-address 192.168.41.101 255.255.255.255
  9 match protocol ssh source-address 192.168.41.102 255.255.255.255
  10 match protocol ssh source-address 192.168.42.111 255.255.255.255
  11 match protocol ssh source-address 192.168.42.122 255.255.255.255
  12 match protocol ssh source-address 192.168.42.124 255.255.255.255
  13 match protocol ssh source-address 192.168.42.131 255.255.255.255
  14 match protocol ssh source-address 192.168.42.133 255.255.255.255
  15 match protocol ssh source-address 192.168.42.138 255.255.255.255
  16 match protocol ssh source-address 192.168.42.139 255.255.255.255
class-map type management match-all V6-MGMT
  2 match protocol icmpv6 anyv6

policy-map type management first-match MGMT
  class MANAGEMENT
    permit
  class V6-MGMT
    permit

policy-map type loadbalance first-match ECOMPOLICY
  class class-default
    serverfarm LAB-ECOM
    nat dynamic 2 vlan 83 serverfarm primary
    insert-http x-forward-for header-value "%is"
```

```
policy-map type loadbalance first-match ECOMPOLICY_v4
  class class-default
    serverfarm LAB-ECOM

policy-map multi-match ECOM_MATCH
  class ECOMVIP
    loadbalance vip inservice
    loadbalance policy ECOMPOLICY
    loadbalance vip icmp-reply active
  class ECOMVIP_v4
    loadbalance vip inservice
    loadbalance policy ECOMPOLICY_v4
    loadbalance vip icmp-reply active

interface vlan 82
  description ACE_outside
  ipv6 enable
  ip address 2001:db8:192:20a4::28/64
  ip address 192.168.20.28 255.255.255.248
  alias 192.168.20.30 255.255.255.248
  peer ip address 192.168.20.29 255.255.255.248
  access-group input out2in
  access-group input out2in_ipv6
  service-policy input ECOM_MATCH
  service-policy input MGMT
  no shutdown
interface vlan 83
  description ACE_inside
  ip address 192.168.20.4 255.255.255.248
  alias 192.168.20.6 255.255.255.248
  peer ip address 192.168.20.5 255.255.255.248
  access-group input in2out
  nat-pool 2 192.168.20.3 192.168.20.3 netmask 255.255.255.248
  no shutdown

domain cisco-irn.com

ip route 0.0.0.0 0.0.0.0 192.168.20.25
ip route ::/0 2001:db8:192:20a4::25


username csmadmin password 5 <removed>  role Admin domain default-domain cisco-irn.com
username bmcgloth password 5 <removed>  role Admin domain default-domain cisco-irn.com
username lmsadmin password 5 <removed>  role Admin domain default-domain cisco-irn.com
```

RIE-3

```
version 15.1
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
service counters max age 5
!
hostname RIE-3
!
boot-start-marker
boot system flash disk0:/s72033-adventerprisek9-mz.151-1.SY.bin
```

```
boot-end-marker
!
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 51200
logging cns-events
enable secret 5 <removed>
enable password 7 <removed>
!

username bart privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
aaa new-model
!
!
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
!
!
!
aaa session-id common
svclc multiple-vlan-interfaces
svclc module 3 vlan-group 21,82,83,85
svclc vlan-group 21  21
svclc vlan-group 82  82
svclc vlan-group 83  83
svclc vlan-group 85  85
firewall multiple-vlan-interfaces
firewall module 7 vlan-group 21,82,200,300
firewall vlan-group 200  22,2305-2307
firewall vlan-group 300  91,92
intrusion-detection module 2 management-port access-vlan 21
intrusion-detection module 2 data-port 1 trunk allowed-vlan 21,83,84,421
clock timezone PST -8
clock summer-time PSTDST recurring
vtp mode transparent
!
!
no ip bootp server
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
ipv6 multicast rpf use-bgp
mls netflow interface
no mls acl tcam share-global
mls cef error action freeze
password encryption aes
!
crypto pki trustpoint TP-self-signed-1014
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1014
 revocation-check none
```

```
 rsakeypair TP-self-signed-1014
!
!
crypto pki certificate chain TP-self-signed-1014
 certificate self-signed 01
  3082023F 308201A8 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  2B312930 27060355 04031320 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 31303134 301E170D 31313032 31323030 35393332 5A170D32
  30303130 31303030 3030305A 302B3129 30270603 55040313 20494F53 2D53656C
  662D5369 676E6564 2D436572 74696669 63617465 2D313031 3430819F 300D0609
  2A864886 F70D0101 01050003 818D0030 81890281 8100BD3E 21BA6626 B7F82E4E
  6B794439 27C36926 27B198DA D92E879D A437284D 4076D650 F671EA49 CC7A9DA4
  BC96B207 7807450D A55F5A9B 85CACE8E E9B85199 B84525E5 FBC82F1D 733A1942
  C47E1F87 87E1026B CD22859C 52307096 B3A6EEEB BCCB3C20 7F39EBCF 6729C4FC
  A13306CF 90815A20 CFA00678 E0856486 3BC8BB88 D51D0203 010001A3 73307130
  0F060355 1D130101 FF040530 030101FF 301E0603 551D1104 17301582 13524945
  2D332E63 6973636F 2D69726E 2E636F6D 301F0603 551D2304 18301680 14E7FF36
  6947643E 752F921F 7674D7DE F1370E50 C6301D06 03551D0E 04160414 E7FF3669
  47643E75 2F921F76 74D7DEF1 370E50C6 300D0609 2A864886 F70D0101 04050003
  81810080 3C7C2250 36EB62DD 12772E91 E3A2CB7D 3D175E31 611404A1 947D97EA
  37E4A5B5 8E888072 B765C977 08C0108C 34FD4AE5 D642F10D 839BE779 F6F2E03F
  581EC8E1 012FA710 583A0E9E B97CCFC0 16AB39CE B8E7A5AB E42C38EB 33CD9F4C
  1D9D5666 1EF8DC52 22C084B1 1C33DB38 0C9E2045 6EBD8BCD B779B172 0B5BE8F5 E5D9DB
        quit
!
!
!
!
!
!
!
!
no power enable module 4
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
diagnostic bootup level minimal
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
!
spanning-tree mode pvst
spanning-tree extend system-id
!
redundancy
 main-cpu
  auto-sync running-config
```

```
 mode sso
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
vlan 21
 name asasm_inside
!
vlan 22
 name asasm_outside
!
vlan 82
 name asasm_Loadbalance_top
!
vlan 83
 name Loadbalance_bottom
!
vlan 84
 name Servers
!
vlan 85
 name Loadbalance_sync
!
vlan 91
 name asasm_failover
!
vlan 92
 name asasm_statelink
!
vlan 421
 name ASASM-to-IDSM
!
vlan 993
 name Management
!
vlan 995
 name DMZ_Management
!
vlan 2305
 name asasm_EmailSecurityAppliance
!
vlan 2306
 name asasm_EmailSecurityMgrAppliance
!
vlan 2307
 name asasm_WebSecApp
!
ip ssh version 2
ip scp server enable
!
!
!
!
!
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key <removed> address 128.107.147.109
!
!
crypto ipsec transform-set to_fred esp-des esp-md5-hmac
 mode tunnel
!
!
!
```

```
crypto map myvpn 10 ipsec-isakmp
 set peer 128.107.147.109
 set transform-set to_fred
 match address 101
!
!
!
!
!
interface Port-channel99
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Tunnel0
 ip address 172.26.0.1 255.255.255.0
 tunnel source Vlan21
 tunnel destination 128.107.147.109
!
interface GigabitEthernet1/1
 description RIE-1 G0/1
 switchport
 switchport access vlan 22
!
interface GigabitEthernet1/2
 description RIE-2 G0/1
 switchport
 switchport access vlan 22
!
interface GigabitEthernet1/3
 no ip address
!
interface GigabitEthernet1/4
 no ip address
!
interface GigabitEthernet1/5
 description ASA-IE-1 G0
 switchport
 switchport access vlan 21
!
interface GigabitEthernet1/6
 no ip address
!
interface GigabitEthernet1/7
 no ip address
!
interface GigabitEthernet1/8
 no ip address
!
interface GigabitEthernet1/9
 no ip address
!
interface GigabitEthernet1/10
 no ip address
!
interface GigabitEthernet1/11
 no ip address
!
interface GigabitEthernet1/12
 no ip address
!
interface GigabitEthernet1/13
 description ESA-IE-1 port M
 switchport
```

```
 switchport access vlan 2306
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet1/14
 description ESA-IE-1 port D1
 switchport
 switchport access vlan 2306
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet1/15
 description ESA-IE-1 port D2
 switchport
 switchport access vlan 2306
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet1/16
 description ESA-IE-1 port D3
 switchport
 switchport access vlan 2306
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet1/17
 description WSA-IE-1 port P1
 no ip address
!
interface GigabitEthernet1/18
 description WSA-IE-1 port P2
 no ip address
!
interface GigabitEthernet1/19
 description WSA-IE-1 port T1
 no ip address
!
interface GigabitEthernet1/20
 description WSA-IE-1 port T2
 no ip address
!
interface GigabitEthernet1/21
 description ESA-IE-1 port M
 switchport
 switchport access vlan 2305
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet1/22
 description ESA-IE-1 port D1
 switchport
 switchport access vlan 2305
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet1/23
 description ESA-IE-1 port D2
 switchport
 switchport access vlan 2305
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet1/24
 description ESA-IE-1 port D3
```

```
 switchport
 switchport access vlan 2305
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet1/25
 description WSA-IE-1 port M
 switchport
 switchport access vlan 2307
 switchport mode access
 spanning-tree portfast edge
!
interface GigabitEthernet1/26
 no ip address
!
interface GigabitEthernet1/27
 no ip address
!
interface GigabitEthernet1/28
 no ip address
!
interface GigabitEthernet1/29
 no ip address
!
interface GigabitEthernet1/30
 no ip address
!
interface GigabitEthernet1/31
 no ip address
!
interface GigabitEthernet1/32
 no ip address
!
interface GigabitEthernet1/33
 no ip address
!
interface GigabitEthernet1/34
 no ip address
!
interface GigabitEthernet1/35
 no ip address
!
interface GigabitEthernet1/36
 no ip address
!
interface GigabitEthernet1/37
 no ip address
!
interface GigabitEthernet1/38
 no ip address
!
interface GigabitEthernet1/39
 no ip address
!
interface GigabitEthernet1/40
 no ip address
!
interface GigabitEthernet1/41
 no ip address
!
interface GigabitEthernet1/42
 no ip address
!
interface GigabitEthernet1/43
```

```
 no ip address
!
interface GigabitEthernet1/44
 no ip address
!
interface GigabitEthernet1/45
 no ip address
!
interface GigabitEthernet1/46
 no ip address
!
interface GigabitEthernet1/47
 description UPLINK from SIE-1
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/48
 description UPLINK from SIE-2
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet5/1
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 99 mode active
!
interface GigabitEthernet5/2
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 99 mode active
!
interface Vlan1
 no ip address
!
interface Vlan21
 description RIE-3 Management
 ip address 192.168.21.91 255.255.255.0
 crypto map myvpn
!
no ip forward-protocol nd
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication CiscoACS
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha rc4-128-sha
ip http timeout-policy idle 60 life 86400 requests 10000
!
!
ip route 0.0.0.0 0.0.0.0 192.168.21.10
ip route 10.10.0.0 255.255.0.0 192.168.21.1
ip route 10.10.0.0 255.255.252.0 192.168.21.10
ip route 10.10.192.0 255.255.240.0 172.26.0.2
ip route 192.168.0.0 255.255.0.0 192.168.21.1
ip route 192.168.23.0 255.255.255.0 192.168.21.10
ip tacacs source-interface Vlan21
!
!
logging trap debugging
logging source-interface Vlan21
logging host 192.168.42.124
```

```
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 192.168.42.139 log
access-list 23 permit 10.19.151.104 log
access-list 23 permit 10.19.151.102 log
access-list 23 permit 10.19.151.103 log
access-list 23 permit 10.19.151.100 log
access-list 23 permit 10.19.151.101 log
access-list 23 permit 10.19.151.98 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.122 log
access-list 88 deny   any log
access-list 101 permit gre host 192.168.21.91 host 128.107.147.109
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  23
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps energywise
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps port-security
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps hsrp
snmp-server enable traps mac-notification move threshold change
snmp-server enable traps ipsla
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps errdisable
snmp-server host 192.168.42.124 <removed>
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
!
!
control-plane
!
!
dial-peer cor custom
!
banner exec ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
```

```
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication CiscoACS
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
!
!
scheduler allocate 20000 1000
ntp source Vlan21
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162
!
end
```

Clinic

Hospital

R-A2-LRG-1

```
version 15.1
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
!
hostname R-A2-Lrg-1
!
boot-start-marker
boot system flash0 c3900-universalk9-mz.SPA.151-3.T.bin
boot-end-marker
!
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 50000
no logging rate-limit
enable secret 5 <removed>
!
aaa new-model
!
!
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default
 action-type start-stop
 group tacacs+
!
aaa accounting commands 15 default
 action-type start-stop
 group tacacs+
!
aaa accounting system default
 action-type start-stop
 group tacacs+
!
!
!
!
!
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PST recurring
!
crypto pki token default removal timeout 0
```

```
!
crypto pki trustpoint TP-self-signed-72006796
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-72006796
 revocation-check none
!
!
crypto pki certificate chain TP-self-signed-72006796
 certificate self-signed 03
  <removed>
    quit
no ipv6 cef
no ip source-route
ip cef
!
!
!
ip multicast-routing
!
!
no ip bootp server
ip domain name cisco-irn.com
ip name-server 192.168.42.130
ip port-map user-8443 port tcp 8443
ip inspect log drop-pkt
ip inspect audit-trail
ip ips config location flash0: retries 1 timeout 1
ip ips name Store-IPS
!
ip ips signature-category
  category all
   retired true
  category ios_ips default
   retired false
!
ip wccp 61
ip wccp 62
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
multilink bundle-name authenticated
!
parameter-map type inspect global
 WAAS enable
parameter-map type inspect Inspect-1
 audit-trail on

parameter-map type trend-global trend-glob-map
!
!
!
!
password encryption aes
voice-card 0
!
!
!
!
!
!
!
license udi pid C3900-SPE150/K9 sn <removed>
```

```
hw-module pvdm 0/0
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
object-group network ActiveDirectory.cisco-irn.com
 host 192.168.42.130
!
object-group service CAPWAP
 description CAPWAP UDP ports 5246 and 5247
 udp eq 5246
 udp eq 5247
!
object-group service CISCO-WAAS
 description Ports for Cisco WAAS
 tcp eq 4050
!
object-group network EMC-NCM
 description EMC Network Configuration Manager
 host 192.168.42.122
!
object-group network RSA-enVision
 description RSA EnVision Syslog collector and SIM
 host 192.168.42.124
!
object-group network CSM_INLINE_dst_rule_81604380995
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object EMC-NCM
 group-object RSA-enVision
!
object-group network TACACS
 description Csico Secure ACS server for TACACS and Radius
 host 192.168.42.131
!
object-group network RSA-AM
 description RSA Authentication Manager for SecureID
 host 192.168.42.137
!
object-group network NAC-1
 description ISE server for NAC
 host 192.168.42.111
!
object-group network CSM_INLINE_dst_rule_81604381001
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object ActiveDirectory.cisco-irn.com
 group-object TACACS
 group-object RSA-AM
 group-object NAC-1
!
object-group network NAC-2
 host 192.168.42.112
!
object-group network CSM_INLINE_dst_rule_81604381037
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object NAC-2
 group-object NAC-1
!
object-group network DC-ALL
 description All of the Data Center
 192.168.0.0 255.255.0.0
```

```
!
object-group network Branches-ALL
 description all branch networks
 10.10.0.0 255.255.0.0
!
object-group network CSM_INLINE_dst_rule_81604381039
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
!
object-group network WCSManager
 description Wireless Manager
 host 192.168.43.135
!
object-group network DC-Wifi-Controllers
 description Central Wireless Controllers for branchs
 host 192.168.43.21
 host 192.168.43.22
!
object-group network DC-Wifi-MSE
 description Mobility Service Engines
 host 192.168.43.31
 host 192.168.43.32
!
object-group network CSM_INLINE_dst_rule_81604381045
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
!
object-group network PAME-DC-1
 host 192.168.44.111
!
object-group network MSP-DC-1
 description Data Center VSOM
 host 192.168.44.121
!
object-group network CSM_INLINE_dst_rule_81604381049
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object PAME-DC-1
 group-object MSP-DC-1
!
object-group network CSM_INLINE_dst_rule_81604381059
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
!
object-group network CSM_INLINE_dst_rule_81604381067
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
!
object-group network CSM_INLINE_dst_rule_81604381071
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
!
object-group network CSM_INLINE_dst_rule_81604381150
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 10.10.126.0 255.255.255.0
 10.10.110.0 255.255.255.0
!
object-group network CSM_INLINE_dst_rule_81604381152
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
```

```
 10.10.126.0 255.255.255.0
 10.10.110.0 255.255.255.0
!
object-group network DC-Admin
 description DC Admin Systems
 host 192.168.41.101
 host 192.168.41.102
!
object-group network CSManager
 description Cisco Security Manager
 host 192.168.42.133
!
object-group network CSM_INLINE_src_rule_81604380993
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-Admin
 group-object EMC-NCM
 group-object CSManager
!
object-group network DC-POS-Tomax
 description Tomax POS Communication from Store to Data Center
 192.168.52.96 255.255.255.224
!
object-group network DC-POS-SAP
 description SAP POS Communication from Store to Data Center
 192.168.52.144 255.255.255.240
!
object-group network DC-POS-Oracle
 description Oracle POS Communication from Store to Data Center
 192.168.52.128 255.255.255.240
!
object-group network CSM_INLINE_src_rule_81604381021
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-Admin
 group-object DC-POS-Tomax
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
!
object-group network CSM_INLINE_src_rule_81604381023
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-Admin
 group-object DC-POS-Tomax
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
!
object-group network CSM_INLINE_src_rule_81604381041
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
!
object-group network CSM_INLINE_src_rule_81604381043
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
!
object-group network CSM_INLINE_src_rule_81604381047
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object PAME-DC-1
 group-object MSP-DC-1
!
object-group network DC-WAAS
 description WAE Appliances in Data Center
 host 192.168.48.10
 host 192.168.49.10
```

```
 host 192.168.47.11
 host 192.168.47.12
!
object-group network CSM_INLINE_src_rule_81604381051
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-Admin
 group-object DC-WAAS
!
object-group network CSM_INLINE_src_rule_81604381150
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 10.10.126.0 255.255.255.0
 10.10.110.0 255.255.255.0
!
object-group network CSM_INLINE_src_rule_81604381152
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 10.10.126.0 255.255.255.0
 10.10.110.0 255.255.255.0
!
object-group service CSM_INLINE_svc_rule_81604380993
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
!
object-group service CSM_INLINE_svc_rule_81604380995
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 udp eq syslog
 udp eq snmp
 udp eq snmptrap
!
object-group service CSM_INLINE_svc_rule_81604381001
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq tacacs
 udp eq 1812
 udp eq 1813
 tcp eq 389
 tcp eq 636
!
object-group service vCenter-to-ESX4
 description Communication from vCetner to ESX hosts
 tcp eq 5989
 tcp eq 8000
 tcp eq 902
 tcp eq 903
!
object-group service CSM_INLINE_svc_rule_81604381003
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq 22
 group-object vCenter-to-ESX4
!
object-group service ESX-SLP
 description CIM Service Location Protocol (SLP) for VMware systems
 udp eq 427
 tcp eq 427
!
object-group service CSM_INLINE_svc_rule_81604381005
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
```

```
 group-object vCenter-to-ESX4
 group-object ESX-SLP
!
object-group service ORACLE-RMI
 description RMI TCP ports 1300 and 1301-1319.
 tcp range 1300 1319
!
object-group service ORACLE-Weblogic
 description HTTP/RMI and HTTPS/RMI-SSL 7001 & 7002. OracleAQ uses 1521.
 tcp eq 7001
 tcp eq 7002
 tcp eq 1521
!
object-group service ORACLE-WAS
 description RMI/IIOP over 2809  HTTP over 9443 IBM-MQ 1414
 tcp eq 2809
 tcp eq 9443
 tcp eq 1414
!
object-group service ORACLE-OAS
 description OAS uses one port for HTTP and RMI - 12601.
 tcp eq 12601
!
object-group service CSM_INLINE_svc_rule_81604381009
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
 group-object ORACLE-RMI
 group-object ORACLE-Weblogic
 group-object ORACLE-WAS
 group-object ORACLE-OAS
!
object-group service CSM_INLINE_svc_rule_81604381011
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
 group-object ORACLE-RMI
 group-object ORACLE-Weblogic
 group-object ORACLE-WAS
 group-object ORACLE-OAS
!
object-group service HTTPS-8443
 tcp eq 8443
!
object-group service CSM_INLINE_svc_rule_81604381013
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
 group-object HTTPS-8443
!
object-group service CSM_INLINE_svc_rule_81604381015
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
 group-object HTTPS-8443
!
object-group service TOMAX-8990
 description Tomax Application Port
 tcp eq 8990
!
```

```
object-group service CSM_INLINE_svc_rule_81604381017
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 group-object TOMAX-8990
!
object-group service CSM_INLINE_svc_rule_81604381019
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 group-object TOMAX-8990
!
object-group service ICMP-Requests
 description ICMP requests
 icmp information-request
 icmp mask-request
 icmp timestamp-request
!
object-group service CSM_INLINE_svc_rule_81604381021
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
 icmp redirect
 icmp alternate-address
 group-object ICMP-Requests
!
object-group service CSM_INLINE_svc_rule_81604381023
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
 icmp redirect
 icmp alternate-address
 group-object ICMP-Requests
!
object-group service CSM_INLINE_svc_rule_81604381025
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq smtp
 tcp eq pop3
 tcp eq 143
!
object-group service CSM_INLINE_svc_rule_81604381027
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_81604381029
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp
 udp
 tcp eq 443
!
object-group service DNS-Resolving
 description Domain Name Server
```

```
 tcp eq domain
 udp eq domain
!
object-group service CSM_INLINE_svc_rule_81604381035
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 udp eq bootps
 group-object DNS-Resolving
!
object-group service CSM_INLINE_svc_rule_81604381037
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
 group-object HTTPS-8443
!
object-group service CSM_INLINE_svc_rule_81604381039
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
!
object-group service CSM_INLINE_svc_rule_81604381041
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
!
object-group service LWAPP
 description LWAPP UDP ports 12222 and 12223
 udp eq 12222
 udp eq 12223
!
object-group service TFTP
 description Trivial File Transfer
 tcp eq 69
 udp eq tftp
!
object-group service IP-Protocol-97
 description IP protocol 97
 97
!
object-group service CSM_INLINE_svc_rule_81604381043
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq www
 tcp eq 22
 tcp eq telnet
 udp eq isakmp
 group-object CAPWAP
 group-object LWAPP
 group-object TFTP
 group-object IP-Protocol-97
!
object-group service Cisco-Mobility
 description Mobility ports for Wireless
 udp eq 16666
 udp eq 16667
!
```

```
object-group service CSM_INLINE_svc_rule_81604381045
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 udp eq isakmp
 group-object CAPWAP
 group-object LWAPP
 group-object Cisco-Mobility
 group-object IP-Protocol-97
!
object-group service Microsoft-DS-SMB
 description Microsoft-DS Active Directory, Windows shares Microsoft-DS SMB file sharing
 tcp eq 445
!
object-group service CSM_INLINE_svc_rule_81604381051
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp
 tcp eq 139
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_81604381053
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp
 tcp eq 139
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_81604381055
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp
 tcp eq 139
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_81604381057
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp
 tcp-udp eq 5060
 tcp eq 2000
 tcp eq www
 tcp eq 443
 group-object TFTP
!
object-group service CSM_INLINE_svc_rule_81604381059
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp-udp eq 5060
 tcp eq 2000
!
object-group service CSM_INLINE_svc_rule_81604381061
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_81604381063
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
```

```
 tcp eq 443
 tcp eq smtp
 tcp eq pop3
 tcp eq 143
!
object-group service Netbios
 description Netbios Servers
 udp eq netbios-dgm
 udp eq netbios-ns
 tcp eq 139
!
object-group service ORACLE-SIM
 description Oracle Store Inventory Management
 tcp eq 7777
 tcp eq 6003
 tcp range 12401 12500
!
object-group service RDP
 description Windows Remote Desktop
 tcp eq 3389
!
object-group service Workbrain
 tcp eq 8444
!
object-group service CSM_INLINE_svc_rule_81604381065
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq ftp
 tcp eq www
 tcp eq 443
 udp eq 88
 tcp-udp eq 42
 group-object Microsoft-DS-SMB
 group-object Netbios
 group-object ORACLE-SIM
 group-object RDP
 group-object Workbrain
!
object-group network DC-Applications
 description Applications in the Data Center
 192.168.180.0 255.255.254.0
!
object-group network DC-Voice
 description Data Center Voice
 192.168.45.0 255.255.255.0
!
object-group network MS-Update
 description Windows Update Server
 host 192.168.42.150
!
object-group network MSExchange
 description Mail Server
 host 192.168.42.140
!
object-group service NTP
 description NTP Protocols
 tcp eq 123
 udp eq ntp
!
object-group network NTP-Servers
 description NTP Servers
 host 192.168.62.161
 host 162.168.62.162
!
```

```
object-group network BRANCH-POS
 10.10.0.0 255.255.0.0
!
object-group network vSphere-1
 description vSphere server for Lab
 host 192.168.41.102
!

username bart privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
redundancy
!
!
!
!
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh version 2
ip scp server enable
!
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_7
 match protocol http
 match protocol https
 match protocol microsoft-ds
 match protocol ms-sql
 match protocol ms-sql-m
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol oracle
 match protocol oracle-em-vp
 match protocol oraclenames
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_10
 match access-group name CSM_ZBF_CMAP_ACL_10
 match class-map CSM_ZBF_CMAP_PLMAP_7
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_4
 match protocol http
 match protocol https
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_23
 match access-group name CSM_ZBF_CMAP_ACL_23
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_17
 match protocol http
 match protocol https
 match protocol imap3
 match protocol pop3
 match protocol pop3s
 match protocol smtp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_32
 match access-group name CSM_ZBF_CMAP_ACL_32
 match class-map CSM_ZBF_CMAP_PLMAP_17
class-map type inspect match-all CSM_ZBF_CLASS_MAP_11
 match access-group name CSM_ZBF_CMAP_ACL_11
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_14
 match protocol http
 match protocol https
```

```
 match protocol user-8443
class-map type inspect match-all CSM_ZBF_CLASS_MAP_22
 match access-group name CSM_ZBF_CMAP_ACL_22
 match class-map CSM_ZBF_CMAP_PLMAP_14
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_20
 match protocol http
 match protocol https
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
 match protocol ftp
 match protocol ssh
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_33
 match access-group name CSM_ZBF_CMAP_ACL_33
 match class-map CSM_ZBF_CMAP_PLMAP_20
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_8
 match protocol sip
 match protocol sip-tls
 match protocol skinny
 match protocol tftp
 match protocol http
 match protocol https
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_12
 match access-group name CSM_ZBF_CMAP_ACL_12
 match class-map CSM_ZBF_CMAP_PLMAP_8
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_13
 match protocol https
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_21
 match access-group name CSM_ZBF_CMAP_ACL_21
 match class-map CSM_ZBF_CMAP_PLMAP_13
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_19
 match protocol http
 match protocol https
 match protocol icmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_30
 match access-group name CSM_ZBF_CMAP_ACL_30
 match class-map CSM_ZBF_CMAP_PLMAP_19
class-map type inspect match-all CSM_ZBF_CLASS_MAP_13
 match access-group name CSM_ZBF_CMAP_ACL_13
class-map type inspect match-all CSM_ZBF_CLASS_MAP_20
 match access-group name CSM_ZBF_CMAP_ACL_20
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_18
 match protocol http
 match protocol https
 match protocol udp
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_31
 match access-group name CSM_ZBF_CMAP_ACL_31
 match class-map CSM_ZBF_CMAP_PLMAP_18
class-map match-all BRANCH-BULK-DATA
 match protocol tftp
 match protocol nfs
 match access-group name BULK-DATA-APPS
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_5
 match protocol http
 match protocol https
 match protocol netbios-dgm
```

```
 match protocol netbios-ns
 match protocol netbios-ssn
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_14
 match access-group name CSM_ZBF_CMAP_ACL_14
 match class-map CSM_ZBF_CMAP_PLMAP_5
class-map type inspect match-all CSM_ZBF_CLASS_MAP_27
 match access-group name CSM_ZBF_CMAP_ACL_27
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_36
 match access-group name CSM_ZBF_CMAP_ACL_36
class-map type inspect match-all CSM_ZBF_CLASS_MAP_15
 match access-group name CSM_ZBF_CMAP_ACL_15
class-map type inspect match-all CSM_ZBF_CLASS_MAP_26
 match access-group name CSM_ZBF_CMAP_ACL_26
 match class-map CSM_ZBF_CMAP_PLMAP_7
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_21
 match protocol tcp
 match protocol udp
 match protocol http
 match protocol https
class-map type inspect match-all CSM_ZBF_CLASS_MAP_37
 match access-group name CSM_ZBF_CMAP_ACL_37
 match class-map CSM_ZBF_CMAP_PLMAP_21
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_9
 match protocol syslog
 match protocol syslog-conn
 match protocol snmp
 match protocol snmptrap
class-map type inspect match-all CSM_ZBF_CLASS_MAP_16
 match access-group name CSM_ZBF_CMAP_ACL_16
 match class-map CSM_ZBF_CMAP_PLMAP_9
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_16
 match protocol http
 match protocol https
 match protocol isakmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_25
 match access-group name CSM_ZBF_CMAP_ACL_25
 match class-map CSM_ZBF_CMAP_PLMAP_16
class-map type inspect match-all CSM_ZBF_CLASS_MAP_34
 match access-group name CSM_ZBF_CMAP_ACL_34
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_10
 match protocol ldaps
 match protocol ldap
 match protocol ldap-admin
 match protocol radius
 match protocol tacacs
 match protocol tacacs-ds
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_17
 match access-group name CSM_ZBF_CMAP_ACL_17
 match class-map CSM_ZBF_CMAP_PLMAP_10
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_15
 match protocol http
 match protocol https
 match protocol netbios-ns
 match protocol netbios-dgm
 match protocol netbios-ssn
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_24
```

```
 match access-group name CSM_ZBF_CMAP_ACL_24
 match class-map CSM_ZBF_CMAP_PLMAP_15
class-map type inspect match-all CSM_ZBF_CLASS_MAP_35
 match access-group name CSM_ZBF_CMAP_ACL_35
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_11
 match protocol ntp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_18
 match access-group name CSM_ZBF_CMAP_ACL_18
 match class-map CSM_ZBF_CMAP_PLMAP_11
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_12
 match protocol bootpc
 match protocol bootps
 match protocol udp
 match protocol tcp
 match protocol dns
 match protocol dhcp-failover
class-map type inspect match-all CSM_ZBF_CLASS_MAP_19
 match access-group name CSM_ZBF_CMAP_ACL_19
 match class-map CSM_ZBF_CMAP_PLMAP_12
class-map type inspect match-all CSM_ZBF_CLASS_MAP_29
 match access-group name CSM_ZBF_CMAP_ACL_29
 match class-map CSM_ZBF_CMAP_PLMAP_18
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_22
 match protocol sip
 match protocol sip-tls
 match protocol skinny
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_38
 match access-group name CSM_ZBF_CMAP_ACL_38
 match class-map CSM_ZBF_CMAP_PLMAP_22
class-map type inspect match-all CSM_ZBF_CLASS_MAP_28
 match access-group name CSM_ZBF_CMAP_ACL_28
 match class-map CSM_ZBF_CMAP_PLMAP_17
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_1
 match protocol https
 match protocol ssh
class-map type inspect match-all CSM_ZBF_CLASS_MAP_1
 match access-group name CSM_ZBF_CMAP_ACL_1
 match class-map CSM_ZBF_CMAP_PLMAP_1
class-map type inspect match-all CSM_ZBF_CLASS_MAP_3
 match access-group name CSM_ZBF_CMAP_ACL_3
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_2
 match protocol https
 match protocol http
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_2
 match access-group name CSM_ZBF_CMAP_ACL_2
 match class-map CSM_ZBF_CMAP_PLMAP_2
class-map type inspect match-all CSM_ZBF_CLASS_MAP_5
 match access-group name CSM_ZBF_CMAP_ACL_5
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_3
 match protocol http
 match protocol https
 match protocol ssh
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_4
 match access-group name CSM_ZBF_CMAP_ACL_4
```

```
 match class-map CSM_ZBF_CMAP_PLMAP_3
class-map type inspect match-all CSM_ZBF_CLASS_MAP_7
 match access-group name CSM_ZBF_CMAP_ACL_7
 match class-map CSM_ZBF_CMAP_PLMAP_5
class-map type inspect match-all CSM_ZBF_CLASS_MAP_6
 match access-group name CSM_ZBF_CMAP_ACL_6
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_9
 match access-group name CSM_ZBF_CMAP_ACL_9
 match protocol tcp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_6
 match protocol http
 match protocol https
 match protocol ssh
 match protocol telnet
 match protocol tftp
 match protocol isakmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_8
 match access-group name CSM_ZBF_CMAP_ACL_8
 match class-map CSM_ZBF_CMAP_PLMAP_6
class-map match-all BULK-DATA
 match ip dscp af11  af12
class-map match-all INTERACTIVE-VIDEO
 match ip dscp af41  af42
class-map match-any BRANCH-TRANSACTIONAL-DATA
 match protocol citrix
 match protocol ldap
 match protocol telnet
 match protocol sqlnet
 match protocol http url "*SalesReport*"
 match access-group name TRANSACTIONAL-DATA-APPS
class-map match-all BRANCH-MISSION-CRITICAL
 match access-group name MISSION-CRITICAL-SERVERS
class-map match-all VOICE
 match ip dscp ef
class-map match-all MISSION-CRITICAL-DATA
 match ip dscp 25
class-map match-any BRANCH-NET-MGMT
 match protocol snmp
 match protocol syslog
 match protocol dns
 match protocol icmp
 match protocol ssh
 match access-group name NET-MGMT-APPS
class-map match-all ROUTING
 match ip dscp cs6
class-map match-all SCAVENGER
 match ip dscp cs1
class-map match-all NET-MGMT
 match ip dscp cs2
class-map match-any BRANCH-SCAVENGER
 match protocol gnutella
 match protocol fasttrack
 match protocol kazaa2
class-map match-any CALL-SIGNALING
 match ip dscp cs3
class-map match-all TRANSACTIONAL-DATA
 match ip dscp af21  af22
!
!
policy-map BRANCH-LAN-EDGE-OUT
 class class-default
```

```
policy-map BRANCH-WAN-EDGE
 class VOICE
  priority percent 18
 class INTERACTIVE-VIDEO
  priority percent 15
 class CALL-SIGNALING
  bandwidth percent 5
 class ROUTING
  bandwidth percent 3
 class NET-MGMT
  bandwidth percent 2
 class MISSION-CRITICAL-DATA
  bandwidth percent 15
  random-detect
 class TRANSACTIONAL-DATA
  bandwidth percent 12
  random-detect dscp-based
 class BULK-DATA
  bandwidth percent 4
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 1
 class class-default
  bandwidth percent 25
  random-detect
policy-map type inspect CSM_ZBF_POLICY_MAP_18
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_19
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_25
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_16
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_23
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_25
 class type inspect CSM_ZBF_CLASS_MAP_18
```

```
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_32
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_36
  drop log
 class type inspect CSM_ZBF_CLASS_MAP_37
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_17
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_24
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_24
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_34
  drop log
 class type inspect CSM_ZBF_CLASS_MAP_35
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_14
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_27
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_15
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
```

```
 class type inspect CSM_ZBF_CLASS_MAP_21
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_26
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_38
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_12
 class type inspect CSM_ZBF_CLASS_MAP_15
  pass
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_21
 class type inspect CSM_ZBF_CLASS_MAP_27
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_28
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_29
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_13
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_20
 class type inspect CSM_ZBF_CLASS_MAP_26
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_27
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_28
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_29
```

```
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_10
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_23
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_31
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_32
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_33
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_11
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_22
 class type inspect CSM_ZBF_CLASS_MAP_30
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_9
 class type inspect CSM_ZBF_CLASS_MAP_13
  pass
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_8
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_12
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_7
 class type inspect CSM_ZBF_CLASS_MAP_9
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_10
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_11
  inspect Inspect-1
```

```
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_6
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_5
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_8
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_4
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_7
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_3
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_5
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_2
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_4
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_1
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_2
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop
policy-map BRANCH-LAN-EDGE-IN
 class BRANCH-MISSION-CRITICAL
  set ip dscp 25
 class BRANCH-TRANSACTIONAL-DATA
  set ip dscp af21
 class BRANCH-NET-MGMT
  set ip dscp cs2
 class BRANCH-BULK-DATA
```

```
  set ip dscp af11
 class BRANCH-SCAVENGER
  set ip dscp cs1
!
zone security S_WAN
 description Store WAN Link
zone security S_R-2-R
 description Bridge link between routers
zone security LOOPBACK
 description Loopback interface
zone security S_MGMT
 description VLAN1000 Management
zone security S_Security
 description VLAN20 Physical Security Systems
zone security S_WAAS
 description VLAN19 WAAS optimization
zone security S_WLC-AP
 description VLAN18 Wireless Systems
zone security S_Data
 description VLAN12 Store Data
zone security S_Data-W
 description VLAN14 Store Wireless Data
zone security S_Guest
 description VLAN17 Guest/Public Wireless
zone security S_Voice
 description VLAN13 Store Voice
zone security S_Partners
 description VLAN16 Partner network
zone security S_POS
 description VLAN 11 POS Data
zone security S_POS-W
 description VLAN15 Store Wireless POS
zone security S_HIPAA
 description VLAN21 HIPAA
zone security S_HIPAA-WU
 description VLAN15 Wireless HIPAA Users
zone security S_HIPAA-WD
 description VLAN15 Wireless HIPAA Devices
zone-pair security CSM_S_WAN-LOOPBACK_1 source S_WAN destination LOOPBACK
 service-policy type inspect CSM_ZBF_POLICY_MAP_1
zone-pair security CSM_S_WAN-S_MGMT_1 source S_WAN destination S_MGMT
 service-policy type inspect CSM_ZBF_POLICY_MAP_2
zone-pair security CSM_S_WAN-S_Security_1 source S_WAN destination S_Security
 service-policy type inspect CSM_ZBF_POLICY_MAP_3
zone-pair security CSM_S_WAN-S_WAAS_1 source S_WAN destination S_WAAS
 service-policy type inspect CSM_ZBF_POLICY_MAP_4
zone-pair security CSM_S_WAN-S_WLC-AP_1 source S_WAN destination S_WLC-AP
 service-policy type inspect CSM_ZBF_POLICY_MAP_5
zone-pair security CSM_S_WAN-S_Data_1 source S_WAN destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Data-W_1 source S_WAN destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Guest_1 source S_WAN destination S_Guest
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Partners_1 source S_WAN destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_POS_1 source S_WAN destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_POS-W_1 source S_WAN destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_HIPAA_1 source S_WAN destination S_HIPAA
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_HIPAA-WU_1 source S_WAN destination S_HIPAA-WU
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
```

```
zone-pair security CSM_S_WAN-S_Voice_1 source S_WAN destination S_Voice
 service-policy type inspect CSM_ZBF_POLICY_MAP_8
zone-pair security CSM_S_R-2-R-LOOPBACK_1 source S_R-2-R destination LOOPBACK
 service-policy type inspect CSM_ZBF_POLICY_MAP_1
zone-pair security CSM_S_R-2-R-S_MGMT_1 source S_R-2-R destination S_MGMT
 service-policy type inspect CSM_ZBF_POLICY_MAP_2
zone-pair security CSM_S_R-2-R-S_Security_1 source S_R-2-R destination S_Security
 service-policy type inspect CSM_ZBF_POLICY_MAP_3
zone-pair security CSM_S_R-2-R-S_WAAS_1 source S_R-2-R destination S_WAAS
 service-policy type inspect CSM_ZBF_POLICY_MAP_4
zone-pair security CSM_S_R-2-R-S_WLC-AP_1 source S_R-2-R destination S_WLC-AP
 service-policy type inspect CSM_ZBF_POLICY_MAP_5
zone-pair security CSM_S_R-2-R-self_1 source S_R-2-R destination self
 service-policy type inspect CSM_ZBF_POLICY_MAP_9
zone-pair security CSM_S_R-2-R-S_Data_1 source S_R-2-R destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_R-2-R-S_Data-W_1 source S_R-2-R destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_R-2-R-S_Guest_1 source S_R-2-R destination S_Guest
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_R-2-R-S_Partners_1 source S_R-2-R destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_R-2-R-S_POS_1 source S_R-2-R destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_R-2-R-S_POS-W_1 source S_R-2-R destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_R-2-R-S_HIPAA_1 source S_R-2-R destination S_HIPAA
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_R-2-R-S_HIPAA-WU_1 source S_R-2-R destination S_HIPAA-WU
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_R-2-R-S_Voice_1 source S_R-2-R destination S_Voice
 service-policy type inspect CSM_ZBF_POLICY_MAP_11
zone-pair security CSM_self-S_R-2-R_1 source self destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_12
zone-pair security CSM_LOOPBACK-S_WAN_1 source LOOPBACK destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_13
zone-pair security CSM_LOOPBACK-S_R-2-R_1 source LOOPBACK destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_13
zone-pair security CSM_LOOPBACK-S_POS_1 source LOOPBACK destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_LOOPBACK-S_POS-W_1 source LOOPBACK destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_MGMT-S_WAN_1 source S_MGMT destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_15
zone-pair security CSM_S_MGMT-S_R-2-R_1 source S_MGMT destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_15
zone-pair security CSM_S_MGMT-S_POS_1 source S_MGMT destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_MGMT-S_POS-W_1 source S_MGMT destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Security-S_WAN_1 source S_Security destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_16
zone-pair security CSM_S_Security-S_R-2-R_1 source S_Security destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_16
zone-pair security CSM_S_Security-S_POS_1 source S_Security destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Security-S_POS-W_1 source S_Security destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_WAN_1 source S_WAAS destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_17
zone-pair security CSM_S_WAAS-S_R-2-R_1 source S_WAAS destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_17
zone-pair security CSM_S_WAAS-S_POS_1 source S_WAAS destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
```

```
zone-pair security CSM_S_WAAS-S_POS-W_1 source S_WAAS destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_Data_1 source S_WAAS destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
zone-pair security CSM_S_WAAS-S_Data-W_1 source S_WAAS destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
zone-pair security CSM_S_WAAS-S_Partners_1 source S_WAAS destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
zone-pair security CSM_S_WLC-AP-S_WAN_1 source S_WLC-AP destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_19
zone-pair security CSM_S_WLC-AP-S_R-2-R_1 source S_WLC-AP destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_19
zone-pair security CSM_S_WLC-AP-S_POS_1 source S_WLC-AP destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WLC-AP-S_POS-W_1 source S_WLC-AP destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_POS-S_WAN_1 source S_POS destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_20
zone-pair security CSM_S_POS-S_R-2-R_1 source S_POS destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_20
zone-pair security CSM_S_POS-W-S_WAN_1 source S_POS-W destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_21
zone-pair security CSM_S_POS-W-S_R-2-R_1 source S_POS-W destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_21
zone-pair security CSM_S_POS-W-S_POS_1 source S_POS-W destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_22
zone-pair security CSM_S_Data-S_POS_1 source S_Data destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Data-S_POS-W_1 source S_Data destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Data-S_WAN_1 source S_Data destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_23
zone-pair security CSM_S_Data-S_R-2-R_1 source S_Data destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_23
zone-pair security CSM_S_Data-W-S_POS_1 source S_Data-W destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Data-W-S_POS-W_1 source S_Data-W destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Data-W-S_WAN_1 source S_Data-W destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_23
zone-pair security CSM_S_Data-W-S_R-2-R_1 source S_Data-W destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_23
zone-pair security CSM_S_Guest-S_POS_1 source S_Guest destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Guest-S_POS-W_1 source S_Guest destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Guest-S_WAN_1 source S_Guest destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_24
zone-pair security CSM_S_Guest-S_R-2-R_1 source S_Guest destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_24
zone-pair security CSM_S_Partners-S_POS_1 source S_Partners destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Partners-S_POS-W_1 source S_Partners destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Partners-S_WAN_1 source S_Partners destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_25
zone-pair security CSM_S_Partners-S_R-2-R_1 source S_Partners destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_25
zone-pair security CSM_S_Voice-S_POS_1 source S_Voice destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Voice-S_POS-W_1 source S_Voice destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Voice-S_WAN_1 source S_Voice destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_26
```

```
zone-pair security CSM_S_Voice-S_R-2-R_1 source S_Voice destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_27
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.10.110.1 255.255.255.255
 ip pim sparse-dense-mode
 zone-member security LOOPBACK
!
interface GigabitEthernet0/0
 description ROUTER LINK TO SWITCH
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.11
 description POS
 encapsulation dot1Q 11
 ip address 10.10.96.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip helper-address 192.168.42.111
 ip pim sparse-dense-mode
 ip ips Store-IPS in
 ip ips Store-IPS out
 zone-member security S_POS
 standby 11 ip 10.10.96.1
 standby 11 priority 101
 standby 11 preempt
 ip igmp query-interval 125
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.12
 description DATA
 encapsulation dot1Q 12
 ip address 10.10.97.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip wccp 61 redirect in
 ip pim sparse-dense-mode
 zone-member security S_Data
 standby 12 ip 10.10.97.1
 standby 12 priority 101
 standby 12 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.13
 description VOICE
 encapsulation dot1Q 13
 ip address 10.10.98.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_Voice
 standby 13 ip 10.10.98.1
 standby 13 priority 101
 standby 13 preempt
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.14
```

```
 description WIRELESS
 encapsulation dot1Q 14
 ip address 10.10.99.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Data-W
 standby 14 ip 10.10.99.1
 standby 14 priority 101
 standby 14 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.15
 description WIRELESS-POS
 encapsulation dot1Q 15
 ip address 10.10.100.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip ips Store-IPS in
 ip ips Store-IPS out
 zone-member security S_POS-W
 standby 15 ip 10.10.100.1
 standby 15 priority 101
 standby 15 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.16
 description PARTNER
 encapsulation dot1Q 16
 ip address 10.10.101.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Partners
 standby 16 ip 10.10.101.1
 standby 16 priority 101
 standby 16 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.17
 description WIRELESS-GUEST
 encapsulation dot1Q 17
 ip address 10.10.102.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Guest
 standby 17 ip 10.10.102.1
 standby 17 priority 101
 standby 17 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.18
 description WIRELESS-CONTROL
 encapsulation dot1Q 18
 ip address 10.10.103.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_WLC-AP
 standby 18 ip 10.10.103.1
 standby 18 priority 101
 standby 18 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.19
 description WAAS
 encapsulation dot1Q 19
```

```
 ip address 10.10.104.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_WAAS
 standby 19 ip 10.10.104.1
 standby 19 priority 101
 standby 19 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.20
 description SECURITY-SYSTEMS
 encapsulation dot1Q 20
 ip address 10.10.105.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_Security
 standby 20 ip 10.10.105.1
 standby 20 priority 101
 standby 20 preempt
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.21
 description HIPAA
 encapsulation dot1Q 21
 ip address 10.10.106.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_HIPAA
 standby 21 ip 10.10.106.1
 standby 21 priority 101
 standby 21 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.22
 description WIRELESS-HIPAA-USERS
 encapsulation dot1Q 22
 ip address 10.10.107.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_HIPAA-WU
 standby 22 ip 10.10.107.1
 standby 22 priority 101
 standby 22 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.23
 description WIRELESS-HIPAA-DEVICES
 encapsulation dot1Q 23
 ip address 10.10.108.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_HIPAA-WD
 standby 23 ip 10.10.108.1
 standby 23 priority 101
 standby 23 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.102
 description ROUTER LINK TO
 encapsulation dot1Q 102
 ip address 10.10.110.29 255.255.255.252
```

```
 ip pim sparse-dense-mode
 zone-member security S_R-2-R
 service-policy input BRANCH-LAN-EDGE-IN
!
interface GigabitEthernet0/0.1000
 description MANAGEMENT
 encapsulation dot1Q 1000
 ip address 10.10.111.2 255.255.255.0
 zone-member security S_MGMT
 standby 100 ip 10.10.111.1
 standby 100 priority 101
 standby 100 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/1.101
 description ROUTER LINK TO
 encapsulation dot1Q 101
 ip address 10.10.110.25 255.255.255.252
 ip pim sparse-dense-mode
 zone-member security S_R-2-R
 service-policy input BRANCH-LAN-EDGE-IN
!
interface GigabitEthernet0/2
 ip address 10.10.255.96 255.255.255.0
 ip ips Store-IPS in
 ip ips Store-IPS out
 zone-member security S_WAN
 duplex auto
 speed auto
 service-policy output BRANCH-WAN-EDGE
!
!
router ospf 5
 router-id 10.10.110.1
 redistribute connected subnets
 passive-interface default
 no passive-interface GigabitEthernet0/0.102
 no passive-interface GigabitEthernet0/1.101
 network 10.10.0.0 0.0.255.255 area 10
 default-information originate
!
no ip forward-protocol nd
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication CiscoACS
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip route 0.0.0.0 0.0.0.0 10.10.255.11
ip tacacs source-interface Loopback0
!
ip access-list extended BULK-DATA-APPS
 remark ---File Transfer---
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
 remark ---E-mail traffic---
```

```
 permit tcp any any eq smtp
 permit tcp any any eq pop3
 permit tcp any any eq 143
 remark ---other EDM app protocols---
 permit tcp any any range 3460 3466
 permit tcp any range 3460 3466 any
 remark ---messaging services---
 permit tcp any any eq 2980
 permit tcp any eq 2980 any
 remark ---Microsoft file services---
 permit tcp any any range 137 139
 permit tcp any range 137 139 any
ip access-list extended CSM_ZBF_CMAP_ACL_1
 remark Data Center Mgmt to Devices
 permit object-group CSM_INLINE_svc_rule_81604380993 object-group
CSM_INLINE_src_rule_81604380993 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_10
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381011 object-group DC-POS-Oracle
object-group BRANCH-POS
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381015 object-group DC-POS-SAP object-group
BRANCH-POS
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381019 object-group DC-POS-Tomax
object-group BRANCH-POS
ip access-list extended CSM_ZBF_CMAP_ACL_11
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381021 object-group
CSM_INLINE_src_rule_81604381021 object-group BRANCH-POS
ip access-list extended CSM_ZBF_CMAP_ACL_12
 remark Data Center VOICE (wired and Wireless)
 permit object-group CSM_INLINE_svc_rule_81604381057 object-group DC-Voice object-group
Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_13
 permit ospf object-group CSM_INLINE_src_rule_81604381150 object-group
CSM_INLINE_dst_rule_81604381150
ip access-list extended CSM_ZBF_CMAP_ACL_14
 remark Store WAAS to Clients and Servers
 permit object-group CSM_INLINE_svc_rule_81604381055 object-group Branches-ALL
object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_15
 permit ospf object-group CSM_INLINE_src_rule_81604381152 object-group
CSM_INLINE_dst_rule_81604381152
ip access-list extended CSM_ZBF_CMAP_ACL_16
 remark Syslog and SNMP Alerts
 permit object-group CSM_INLINE_svc_rule_81604380995 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_81604380995
ip access-list extended CSM_ZBF_CMAP_ACL_17
 remark Store to Data Center Authentications
 permit object-group CSM_INLINE_svc_rule_81604381001 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_81604381001
ip access-list extended CSM_ZBF_CMAP_ACL_18
 remark Store to Data Center for NTP
 permit object-group NTP object-group Branches-ALL object-group NTP-Servers
ip access-list extended CSM_ZBF_CMAP_ACL_19
 remark Store to Data Center for DHCP and DNS
 permit object-group CSM_INLINE_svc_rule_81604381035 object-group Branches-ALL
object-group ActiveDirectory.cisco-irn.com
ip access-list extended CSM_ZBF_CMAP_ACL_2
 remark Data Center subscribe to IPS SDEE events
 permit tcp object-group RSA-enVision object-group Branches-ALL eq 443
ip access-list extended CSM_ZBF_CMAP_ACL_20
 remark Permit ICMP traffic
```

```
 permit object-group CSM_INLINE_svc_rule_81604381039 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_81604381039
ip access-list extended CSM_ZBF_CMAP_ACL_21
 remark Store UCS E-series server to Data Center vShphere
 permit object-group CSM_INLINE_svc_rule_81604381005 object-group Branches-ALL
object-group vSphere-1
ip access-list extended CSM_ZBF_CMAP_ACL_22
 remark Store NAC
 permit object-group CSM_INLINE_svc_rule_81604381037 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_81604381037
ip access-list extended CSM_ZBF_CMAP_ACL_23
 remark Store to Data Center Physical Security
 permit ip object-group Branches-ALL object-group CSM_INLINE_dst_rule_81604381049
ip access-list extended CSM_ZBF_CMAP_ACL_24
 remark Store WAAS (WAAS Devices need their own zone)
 permit object-group CSM_INLINE_svc_rule_81604381053 object-group Branches-ALL
object-group DC-WAAS
ip access-list extended CSM_ZBF_CMAP_ACL_25
 remark Store to Data Center wireless controller traffic
 permit object-group CSM_INLINE_svc_rule_81604381045 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_81604381045
ip access-list extended CSM_ZBF_CMAP_ACL_26
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381009 object-group BRANCH-POS object-group
DC-POS-Oracle
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381013 object-group BRANCH-POS object-group
DC-POS-SAP
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381017 object-group BRANCH-POS object-group
DC-POS-Tomax
ip access-list extended CSM_ZBF_CMAP_ACL_27
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381023 object-group
CSM_INLINE_src_rule_81604381023 object-group BRANCH-POS
ip access-list extended CSM_ZBF_CMAP_ACL_28
 remark Store to Data Center for E-mail
 permit object-group CSM_INLINE_svc_rule_81604381025 object-group BRANCH-POS object-group
MSExchange
ip access-list extended CSM_ZBF_CMAP_ACL_29
 remark Store to Data Center for Windows Updates
 permit object-group CSM_INLINE_svc_rule_81604381027 object-group BRANCH-POS object-group
MS-Update
ip access-list extended CSM_ZBF_CMAP_ACL_3
 remark Permit ICMP traffic
 permit object-group CSM_INLINE_svc_rule_81604381041 object-group
CSM_INLINE_src_rule_81604381041 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_30
 remark Permit POS clients to talk to branch POS server
 permit object-group CSM_INLINE_svc_rule_81604381029 object-group BRANCH-POS object-group
BRANCH-POS
ip access-list extended CSM_ZBF_CMAP_ACL_31
 remark Store to Data Center for Windows Updates
 permit object-group CSM_INLINE_svc_rule_81604381061 object-group Branches-ALL
object-group MS-Update
ip access-list extended CSM_ZBF_CMAP_ACL_32
 remark Store to Data Center for E-mail
 permit object-group CSM_INLINE_svc_rule_81604381063 object-group Branches-ALL
object-group MSExchange
ip access-list extended CSM_ZBF_CMAP_ACL_33
 remark Store DATA (wired and Wireless - Access to DC Other applications)
 permit object-group CSM_INLINE_svc_rule_81604381065 object-group Branches-ALL
object-group DC-Applications
ip access-list extended CSM_ZBF_CMAP_ACL_34
```

```
 remark Store GUEST - Drop Traffic to Enterprise
 permit ip object-group Branches-ALL object-group CSM_INLINE_dst_rule_81604381071
ip access-list extended CSM_ZBF_CMAP_ACL_35
 remark Store GUEST (access to internet/DMZ web servers)
 permit ip object-group Branches-ALL any
ip access-list extended CSM_ZBF_CMAP_ACL_36
 remark Store PARTNERS - Drop Traffic to Enterprise
 permit ip object-group Branches-ALL object-group CSM_INLINE_dst_rule_81604381067
ip access-list extended CSM_ZBF_CMAP_ACL_37
 remark Store PARTNERS (wired and wireless - Access to Partner site, Internet VPN)
 permit ip object-group Branches-ALL any
ip access-list extended CSM_ZBF_CMAP_ACL_38
 remark Store VOICE (wired and Wireless - Acess to corporate wide voice)
 permit object-group CSM_INLINE_svc_rule_81604381059 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_81604381059
ip access-list extended CSM_ZBF_CMAP_ACL_4
 remark Data Center vSphere to UCS E-series server
 permit object-group CSM_INLINE_svc_rule_81604381003 object-group vSphere-1 object-group
Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_5
 remark Data Center to Store Physical Security
 permit ip object-group CSM_INLINE_src_rule_81604381047 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_6
 remark Data Center Mgmt to Devices
 permit object-group RDP object-group DC-Admin object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_7
 remark Data Center WAAS to Store
 permit object-group CSM_INLINE_svc_rule_81604381051 object-group
CSM_INLINE_src_rule_81604381051 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_8
 remark Data Center Wireless Control to AP's and Controllers in branchs
 permit object-group CSM_INLINE_svc_rule_81604381043 object-group
CSM_INLINE_src_rule_81604381043 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_9
 remark Data Center Mgmt to Devices
 permit object-group RDP object-group DC-Admin object-group BRANCH-POS
ip access-list extended MISSION-CRITICAL-SERVERS
 remark ---POS Applications---
 permit ip any 192.168.52.0 0.0.0.255
ip access-list extended NET-MGMT-APPS
 remark - Router user Authentication - Identifies TACACS Control traffic
 permit tcp any any eq tacacs
 permit tcp any eq tacacs any
ip access-list extended TRANSACTIONAL-DATA-APPS
 remark ---Workbrain Application---
 remark --Large Store Clock Server to Central Clock Application
 permit tcp host 10.10.49.94 host 192.168.46.72 eq 8444
 remark --Large branch Clock Server to CUAE
 permit tcp host 10.10.49.94 host 192.168.45.185 eq 8000
 remark ---LiteScape Application---
 permit ip any host 192.168.46.82
 permit ip any 239.192.0.0 0.0.0.255
 permit ip any host 239.255.255.250
 remark ---Remote Desktop---
 permit tcp any any eq 3389
 permit tcp any eq 3389 any
 remark ---Oracle SIM---
 permit tcp any 192.168.46.0 0.0.0.255 eq 7777
 permit tcp any 192.168.46.0 0.0.0.255 eq 6003
 permit tcp any 192.168.46.0 0.0.0.255 range 12401 12500
 permit tcp 192.168.46.0 0.0.0.255 eq 7777 any
 permit tcp 192.168.46.0 0.0.0.255 eq 6003 any
 permit tcp 192.168.46.0 0.0.0.255 range 12401 12500 any
!
```

```
logging esm config
logging trap debugging
logging source-interface Loopback0
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
!
!
!
nls resp-timeout 1
cpd cr-id 1
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps flash insertion removal
snmp-server enable traps energywise
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps ipsla
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server domain-stripping
tacacs-server key 7 <removed>
!
!
control-plane
!
!
!
!
mgcp profile default
!
!
!
!
!
```

```
gatekeeper
 shutdown
!
!
banner exec C
WARNING:
**** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
**** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner incoming C
WARNING:
**** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
**** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner login
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!

!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication CiscoACS
line aux 0
 session-timeout 1  output
 exec-timeout 0 1
 privilege level 0
 login authentication CiscoACS
 no exec
 transport preferred none
 transport output none
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
```

```
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162
end
```

R-A2-LRG-2

```
version 15.1
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
!
hostname R-A2-Lrg-2
!
boot-start-marker
boot system flash0 c3900-universalk9-mz.SPA.151-3.T.bin
boot-end-marker
!
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 50000
no logging rate-limit
enable secret 5 <removed>
!
aaa new-model
!
!
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default
 action-type start-stop
 group tacacs+
!
aaa accounting commands 15 default
 action-type start-stop
 group tacacs+
!
aaa accounting system default
 action-type start-stop
 group tacacs+
!
!
!
!
!
```

```
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PST recurring
!
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-660084654
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-660084654
 revocation-check none
 rsakeypair TP-self-signed-660084654
!
!
crypto pki certificate chain TP-self-signed-660084654
 certificate self-signed 01
  <removed>
    quit
no ipv6 cef
no ip source-route
ip cef
!
!
!
ip multicast-routing
!
!
no ip bootp server
ip domain name cisco-irn.com
ip name-server 192.168.42.130
ip port-map user-8443 port tcp 8443
ip inspect log drop-pkt
ip inspect audit-trail
ip ips config location flash0: retries 1 timeout 1
ip ips name Store-IPS
!
ip ips signature-category
  category all
   retired true
  category ios_ips default
   retired false
!
ip wccp 61
ip wccp 62
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
multilink bundle-name authenticated
!
parameter-map type inspect global
 WAAS enable
parameter-map type inspect Inspect-1
 audit-trail on

parameter-map type trend-global trend-glob-map
!
!
!
!
password encryption aes
voice-card 0
```

```
!
!
!
!
!
!
!
license udi pid C3900-SPE150/K9 sn <removed>
hw-module pvdm 0/0
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
object-group network ActiveDirectory.cisco-irn.com
 host 192.168.42.130
!
object-group service CAPWAP
 description CAPWAP UDP ports 5246 and 5247
 udp eq 5246
 udp eq 5247
!
object-group service CISCO-WAAS
 description Ports for Cisco WAAS
 tcp eq 4050
!
object-group network EMC-NCM
 description EMC Network Configuration Manager
 host 192.168.42.122
!
object-group network RSA-enVision
 description RSA EnVision Syslog collector and SIM
 host 192.168.42.124
!
object-group network CSM_INLINE_dst_rule_81604380995
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object EMC-NCM
 group-object RSA-enVision
!
object-group network TACACS
 description Csico Secure ACS server for TACACS and Radius
 host 192.168.42.131
!
object-group network RSA-AM
 description RSA Authentication Manager for SecureID
 host 192.168.42.137
!
object-group network NAC-1
 description ISE server for NAC
 host 192.168.42.111
!
object-group network CSM_INLINE_dst_rule_81604381001
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object ActiveDirectory.cisco-irn.com
 group-object TACACS
 group-object RSA-AM
 group-object NAC-1
!
object-group network NAC-2
 host 192.168.42.112
!
```

```
object-group network CSM_INLINE_dst_rule_81604381037
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object NAC-2
 group-object NAC-1
!
object-group network DC-ALL
 description All of the Data Center
 192.168.0.0 255.255.0.0
!
object-group network Branches-ALL
 description all branch networks
 10.10.0.0 255.255.0.0
!
object-group network CSM_INLINE_dst_rule_81604381039
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
!
object-group network WCSManager
 description Wireless Manager
 host 192.168.43.135
!
object-group network DC-Wifi-Controllers
 description Central Wireless Controllers for branchs
 host 192.168.43.21
 host 192.168.43.22
!
object-group network DC-Wifi-MSE
 description Mobility Service Engines
 host 192.168.43.31
 host 192.168.43.32
!
object-group network CSM_INLINE_dst_rule_81604381045
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
!
object-group network PAME-DC-1
 host 192.168.44.111
!
object-group network MSP-DC-1
 description Data Center VSOM
 host 192.168.44.121
!
object-group network CSM_INLINE_dst_rule_81604381049
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object PAME-DC-1
 group-object MSP-DC-1
!
object-group network CSM_INLINE_dst_rule_81604381059
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
!
object-group network CSM_INLINE_dst_rule_81604381067
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
!
object-group network CSM_INLINE_dst_rule_81604381071
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
```

```
!
object-group network CSM_INLINE_dst_rule_81604381150
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 10.10.126.0 255.255.255.0
 10.10.110.0 255.255.255.0
!
object-group network CSM_INLINE_dst_rule_81604381152
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 10.10.126.0 255.255.255.0
 10.10.110.0 255.255.255.0
!
object-group network DC-Admin
 description DC Admin Systems
 host 192.168.41.101
 host 192.168.41.102
!
object-group network CSManager
 description Cisco Security Manager
 host 192.168.42.133
!
object-group network CSM_INLINE_src_rule_81604380993
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-Admin
 group-object EMC-NCM
 group-object CSManager
!
object-group network DC-POS-Tomax
 description Tomax POS Communication from Store to Data Center
 192.168.52.96 255.255.255.224
!
object-group network DC-POS-SAP
 description SAP POS Communication from Store to Data Center
 192.168.52.144 255.255.255.240
!
object-group network DC-POS-Oracle
 description Oracle POS Communication from Store to Data Center
 192.168.52.128 255.255.255.240
!
object-group network CSM_INLINE_src_rule_81604381021
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-Admin
 group-object DC-POS-Tomax
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
!
object-group network CSM_INLINE_src_rule_81604381023
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-Admin
 group-object DC-POS-Tomax
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
!
object-group network CSM_INLINE_src_rule_81604381041
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
!
object-group network CSM_INLINE_src_rule_81604381043
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
!
object-group network CSM_INLINE_src_rule_81604381047
```

```
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object PAME-DC-1
 group-object MSP-DC-1
!
object-group network DC-WAAS
 description WAE Appliances in Data Center
 host 192.168.48.10
 host 192.168.49.10
 host 192.168.47.11
 host 192.168.47.12
!
object-group network CSM_INLINE_src_rule_81604381051
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-Admin
 group-object DC-WAAS
!
object-group network CSM_INLINE_src_rule_81604381150
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 10.10.126.0 255.255.255.0
 10.10.110.0 255.255.255.0
!
object-group network CSM_INLINE_src_rule_81604381152
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 10.10.126.0 255.255.255.0
 10.10.110.0 255.255.255.0
!
object-group service CSM_INLINE_svc_rule_81604380993
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
!
object-group service CSM_INLINE_svc_rule_81604380995
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 udp eq syslog
 udp eq snmp
 udp eq snmptrap
!
object-group service CSM_INLINE_svc_rule_81604381001
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq tacacs
 udp eq 1812
 udp eq 1813
 tcp eq 389
 tcp eq 636
!
object-group service vCenter-to-ESX4
 description Communication from vCetner to ESX hosts
 tcp eq 5989
 tcp eq 8000
 tcp eq 902
 tcp eq 903
!
object-group service CSM_INLINE_svc_rule_81604381003
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq 22
 group-object vCenter-to-ESX4
!
object-group service ESX-SLP
```

```
 description CIM Service Location Protocol (SLP) for VMware systems
 udp eq 427
 tcp eq 427
!
object-group service CSM_INLINE_svc_rule_81604381005
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 group-object vCenter-to-ESX4
 group-object ESX-SLP
!
object-group service ORACLE-RMI
 description RMI TCP ports 1300 and 1301-1319.
 tcp range 1300 1319
!
object-group service ORACLE-Weblogic
 description HTTP/RMI and HTTPS/RMI-SSL 7001 & 7002. OracleAQ uses 1521.
 tcp eq 7001
 tcp eq 7002
 tcp eq 1521
!
object-group service ORACLE-WAS
 description RMI/IIOP over 2809  HTTP over 9443 IBM-MQ 1414
 tcp eq 2809
 tcp eq 9443
 tcp eq 1414
!
object-group service ORACLE-OAS
 description OAS uses one port for HTTP and RMI - 12601.
 tcp eq 12601
!
object-group service CSM_INLINE_svc_rule_81604381009
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
 group-object ORACLE-RMI
 group-object ORACLE-Weblogic
 group-object ORACLE-WAS
 group-object ORACLE-OAS
!
object-group service CSM_INLINE_svc_rule_81604381011
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
 group-object ORACLE-RMI
 group-object ORACLE-Weblogic
 group-object ORACLE-WAS
 group-object ORACLE-OAS
!
object-group service HTTPS-8443
 tcp eq 8443
!
object-group service CSM_INLINE_svc_rule_81604381013
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
 group-object HTTPS-8443
!
object-group service CSM_INLINE_svc_rule_81604381015
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
```

```
 tcp eq 443
 tcp eq 22
 group-object HTTPS-8443
!
object-group service TOMAX-8990
 description Tomax Application Port
 tcp eq 8990
!
object-group service CSM_INLINE_svc_rule_81604381017
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 group-object TOMAX-8990
!
object-group service CSM_INLINE_svc_rule_81604381019
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 group-object TOMAX-8990
!
object-group service ICMP-Requests
 description ICMP requests
 icmp information-request
 icmp mask-request
 icmp timestamp-request
!
object-group service CSM_INLINE_svc_rule_81604381021
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
 icmp redirect
 icmp alternate-address
 group-object ICMP-Requests
!
object-group service CSM_INLINE_svc_rule_81604381023
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
 icmp redirect
 icmp alternate-address
 group-object ICMP-Requests
!
object-group service CSM_INLINE_svc_rule_81604381025
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq smtp
 tcp eq pop3
 tcp eq 143
!
object-group service CSM_INLINE_svc_rule_81604381027
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_81604381029
```

```
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp
 udp
 tcp eq 443
!
object-group service DNS-Resolving
 description Domain Name Server
 tcp eq domain
 udp eq domain
!
object-group service CSM_INLINE_svc_rule_81604381035
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 udp eq bootps
 group-object DNS-Resolving
!
object-group service CSM_INLINE_svc_rule_81604381037
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
 group-object HTTPS-8443
!
object-group service CSM_INLINE_svc_rule_81604381039
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
!
object-group service CSM_INLINE_svc_rule_81604381041
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
!
object-group service LWAPP
 description LWAPP UDP ports 12222 and 12223
 udp eq 12222
 udp eq 12223
!
object-group service TFTP
 description Trivial File Transfer
 tcp eq 69
 udp eq tftp
!
object-group service IP-Protocol-97
 description IP protocol 97
 97
!
object-group service CSM_INLINE_svc_rule_81604381043
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq www
 tcp eq 22
 tcp eq telnet
 udp eq isakmp
 group-object CAPWAP
 group-object LWAPP
```

```
 group-object TFTP
 group-object IP-Protocol-97
!
object-group service Cisco-Mobility
 description Mobility ports for Wireless
 udp eq 16666
 udp eq 16667
!
object-group service CSM_INLINE_svc_rule_81604381045
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 udp eq isakmp
 group-object CAPWAP
 group-object LWAPP
 group-object Cisco-Mobility
 group-object IP-Protocol-97
!
object-group service Microsoft-DS-SMB
 description Microsoft-DS Active Directory, Windows shares Microsoft-DS SMB file sharing
 tcp eq 445
!
object-group service CSM_INLINE_svc_rule_81604381051
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp
 tcp eq 139
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_81604381053
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp
 tcp eq 139
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_81604381055
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp
 tcp eq 139
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_81604381057
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp
 tcp-udp eq 5060
 tcp eq 2000
 tcp eq www
 tcp eq 443
 group-object TFTP
!
object-group service CSM_INLINE_svc_rule_81604381059
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp-udp eq 5060
 tcp eq 2000
!
object-group service CSM_INLINE_svc_rule_81604381061
```

```
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_81604381063
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq smtp
 tcp eq pop3
 tcp eq 143
!
object-group service Netbios
 description Netbios Servers
 udp eq netbios-dgm
 udp eq netbios-ns
 tcp eq 139
!
object-group service ORACLE-SIM
 description Oracle Store Inventory Management
 tcp eq 7777
 tcp eq 6003
 tcp range 12401 12500
!
object-group service RDP
 description Windows Remote Desktop
 tcp eq 3389
!
object-group service Workbrain
 tcp eq 8444
!
object-group service CSM_INLINE_svc_rule_81604381065
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq ftp
 tcp eq www
 tcp eq 443
 udp eq 88
 tcp-udp eq 42
 group-object Microsoft-DS-SMB
 group-object Netbios
 group-object ORACLE-SIM
 group-object RDP
 group-object Workbrain
!
object-group network DC-Applications
 description Applications in the Data Center
 192.168.180.0 255.255.254.0
!
object-group network DC-Voice
 description Data Center Voice
 192.168.45.0 255.255.255.0
!
object-group network MS-Update
 description Windows Update Server
 host 192.168.42.150
!
object-group network MSExchange
 description Mail Server
 host 192.168.42.140
!
object-group service NTP
```

```
 description NTP Protocols
 tcp eq 123
 udp eq ntp
!
object-group network NTP-Servers
 description NTP Servers
 host 192.168.62.161
 host 162.168.62.162
!
object-group network BRANCH-POS
 10.10.0.0 255.255.0.0
!
object-group network vSphere-1
 description vSphere server for Lab
 host 192.168.41.102
!

username bart privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
redundancy
!
!
!
!
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh version 2
ip scp server enable
!
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_7
 match protocol http
 match protocol https
 match protocol microsoft-ds
 match protocol ms-sql
 match protocol ms-sql-m
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol oracle
 match protocol oracle-em-vp
 match protocol oraclenames
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_10
 match access-group name CSM_ZBF_CMAP_ACL_10
 match class-map CSM_ZBF_CMAP_PLMAP_7
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_4
 match protocol http
 match protocol https
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_23
 match access-group name CSM_ZBF_CMAP_ACL_23
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_17
 match protocol http
 match protocol https
 match protocol imap3
 match protocol pop3
 match protocol pop3s
 match protocol smtp
 match protocol tcp
 match protocol udp
```

```
class-map type inspect match-all CSM_ZBF_CLASS_MAP_32
 match access-group name CSM_ZBF_CMAP_ACL_32
 match class-map CSM_ZBF_CMAP_PLMAP_17
class-map type inspect match-all CSM_ZBF_CLASS_MAP_11
 match access-group name CSM_ZBF_CMAP_ACL_11
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_14
 match protocol http
 match protocol https
 match protocol user-8443
class-map type inspect match-all CSM_ZBF_CLASS_MAP_22
 match access-group name CSM_ZBF_CMAP_ACL_22
 match class-map CSM_ZBF_CMAP_PLMAP_14
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_20
 match protocol http
 match protocol https
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
 match protocol ftp
 match protocol ssh
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_33
 match access-group name CSM_ZBF_CMAP_ACL_33
 match class-map CSM_ZBF_CMAP_PLMAP_20
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_8
 match protocol sip
 match protocol sip-tls
 match protocol skinny
 match protocol tftp
 match protocol http
 match protocol https
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_12
 match access-group name CSM_ZBF_CMAP_ACL_12
 match class-map CSM_ZBF_CMAP_PLMAP_8
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_13
 match protocol https
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_21
 match access-group name CSM_ZBF_CMAP_ACL_21
 match class-map CSM_ZBF_CMAP_PLMAP_13
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_19
 match protocol http
 match protocol https
 match protocol icmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_30
 match access-group name CSM_ZBF_CMAP_ACL_30
 match class-map CSM_ZBF_CMAP_PLMAP_19
class-map type inspect match-all CSM_ZBF_CLASS_MAP_13
 match access-group name CSM_ZBF_CMAP_ACL_13
class-map type inspect match-all CSM_ZBF_CLASS_MAP_20
 match access-group name CSM_ZBF_CMAP_ACL_20
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_18
 match protocol http
 match protocol https
 match protocol udp
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_31
 match access-group name CSM_ZBF_CMAP_ACL_31
```

```
 match class-map CSM_ZBF_CMAP_PLMAP_18
class-map match-all BRANCH-BULK-DATA
 match protocol tftp
 match protocol nfs
 match access-group name BULK-DATA-APPS
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_5
 match protocol http
 match protocol https
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_14
 match access-group name CSM_ZBF_CMAP_ACL_14
 match class-map CSM_ZBF_CMAP_PLMAP_5
class-map type inspect match-all CSM_ZBF_CLASS_MAP_27
 match access-group name CSM_ZBF_CMAP_ACL_27
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_36
 match access-group name CSM_ZBF_CMAP_ACL_36
class-map type inspect match-all CSM_ZBF_CLASS_MAP_15
 match access-group name CSM_ZBF_CMAP_ACL_15
class-map type inspect match-all CSM_ZBF_CLASS_MAP_26
 match access-group name CSM_ZBF_CMAP_ACL_26
 match class-map CSM_ZBF_CMAP_PLMAP_7
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_21
 match protocol tcp
 match protocol udp
 match protocol http
 match protocol https
class-map type inspect match-all CSM_ZBF_CLASS_MAP_37
 match access-group name CSM_ZBF_CMAP_ACL_37
 match class-map CSM_ZBF_CMAP_PLMAP_21
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_9
 match protocol syslog
 match protocol syslog-conn
 match protocol snmp
 match protocol snmptrap
class-map type inspect match-all CSM_ZBF_CLASS_MAP_16
 match access-group name CSM_ZBF_CMAP_ACL_16
 match class-map CSM_ZBF_CMAP_PLMAP_9
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_16
 match protocol http
 match protocol https
 match protocol isakmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_25
 match access-group name CSM_ZBF_CMAP_ACL_25
 match class-map CSM_ZBF_CMAP_PLMAP_16
class-map type inspect match-all CSM_ZBF_CLASS_MAP_34
 match access-group name CSM_ZBF_CMAP_ACL_34
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_10
 match protocol ldaps
 match protocol ldap
 match protocol ldap-admin
 match protocol radius
 match protocol tacacs
 match protocol tacacs-ds
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_17
 match access-group name CSM_ZBF_CMAP_ACL_17
 match class-map CSM_ZBF_CMAP_PLMAP_10
```

```
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_15
 match protocol http
 match protocol https
 match protocol netbios-ns
 match protocol netbios-dgm
 match protocol netbios-ssn
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_24
 match access-group name CSM_ZBF_CMAP_ACL_24
 match class-map CSM_ZBF_CMAP_PLMAP_15
class-map type inspect match-all CSM_ZBF_CLASS_MAP_35
 match access-group name CSM_ZBF_CMAP_ACL_35
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_11
 match protocol ntp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_18
 match access-group name CSM_ZBF_CMAP_ACL_18
 match class-map CSM_ZBF_CMAP_PLMAP_11
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_12
 match protocol bootpc
 match protocol bootps
 match protocol udp
 match protocol tcp
 match protocol dns
 match protocol dhcp-failover
class-map type inspect match-all CSM_ZBF_CLASS_MAP_19
 match access-group name CSM_ZBF_CMAP_ACL_19
 match class-map CSM_ZBF_CMAP_PLMAP_12
class-map type inspect match-all CSM_ZBF_CLASS_MAP_29
 match access-group name CSM_ZBF_CMAP_ACL_29
 match class-map CSM_ZBF_CMAP_PLMAP_18
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_22
 match protocol sip
 match protocol sip-tls
 match protocol skinny
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_38
 match access-group name CSM_ZBF_CMAP_ACL_38
 match class-map CSM_ZBF_CMAP_PLMAP_22
class-map type inspect match-all CSM_ZBF_CLASS_MAP_28
 match access-group name CSM_ZBF_CMAP_ACL_28
 match class-map CSM_ZBF_CMAP_PLMAP_17
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_1
 match protocol https
 match protocol ssh
class-map type inspect match-all CSM_ZBF_CLASS_MAP_1
 match access-group name CSM_ZBF_CMAP_ACL_1
 match class-map CSM_ZBF_CMAP_PLMAP_1
class-map type inspect match-all CSM_ZBF_CLASS_MAP_3
 match access-group name CSM_ZBF_CMAP_ACL_3
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_2
 match protocol https
 match protocol http
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_2
 match access-group name CSM_ZBF_CMAP_ACL_2
 match class-map CSM_ZBF_CMAP_PLMAP_2
class-map type inspect match-all CSM_ZBF_CLASS_MAP_5
 match access-group name CSM_ZBF_CMAP_ACL_5
```

```
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_3
 match protocol http
 match protocol https
 match protocol ssh
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_4
 match access-group name CSM_ZBF_CMAP_ACL_4
 match class-map CSM_ZBF_CMAP_PLMAP_3
class-map type inspect match-all CSM_ZBF_CLASS_MAP_7
 match access-group name CSM_ZBF_CMAP_ACL_7
 match class-map CSM_ZBF_CMAP_PLMAP_5
class-map type inspect match-all CSM_ZBF_CLASS_MAP_6
 match access-group name CSM_ZBF_CMAP_ACL_6
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_9
 match access-group name CSM_ZBF_CMAP_ACL_9
 match protocol tcp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_6
 match protocol http
 match protocol https
 match protocol ssh
 match protocol telnet
 match protocol tftp
 match protocol isakmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_8
 match access-group name CSM_ZBF_CMAP_ACL_8
 match class-map CSM_ZBF_CMAP_PLMAP_6
class-map match-all BULK-DATA
 match ip dscp af11  af12
class-map match-all INTERACTIVE-VIDEO
 match ip dscp af41  af42
class-map match-any BRANCH-TRANSACTIONAL-DATA
 match protocol citrix
 match protocol ldap
 match protocol telnet
 match protocol sqlnet
 match protocol http url "*SalesReport*"
 match access-group name TRANSACTIONAL-DATA-APPS
class-map match-all BRANCH-MISSION-CRITICAL
 match access-group name MISSION-CRITICAL-SERVERS
class-map match-all VOICE
 match ip dscp ef
class-map match-all MISSION-CRITICAL-DATA
 match ip dscp 25
class-map match-any BRANCH-NET-MGMT
 match protocol snmp
 match protocol syslog
 match protocol dns
 match protocol icmp
 match protocol ssh
 match access-group name NET-MGMT-APPS
class-map match-all ROUTING
 match ip dscp cs6
class-map match-all SCAVENGER
 match ip dscp cs1
class-map match-all NET-MGMT
 match ip dscp cs2
class-map match-any BRANCH-SCAVENGER
 match protocol gnutella
 match protocol fasttrack
```

```
 match protocol kazaa2
class-map match-any CALL-SIGNALING
 match ip dscp cs3
class-map match-all TRANSACTIONAL-DATA
 match ip dscp af21  af22
!
!
policy-map BRANCH-LAN-EDGE-OUT
 class class-default
policy-map BRANCH-WAN-EDGE
 class VOICE
  priority percent 18
 class INTERACTIVE-VIDEO
  priority percent 15
 class CALL-SIGNALING
  bandwidth percent 5
 class ROUTING
  bandwidth percent 3
 class NET-MGMT
  bandwidth percent 2
 class MISSION-CRITICAL-DATA
  bandwidth percent 15
  random-detect
 class TRANSACTIONAL-DATA
  bandwidth percent 12
  random-detect dscp-based
 class BULK-DATA
  bandwidth percent 4
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 1
 class class-default
  bandwidth percent 25
  random-detect
policy-map type inspect CSM_ZBF_POLICY_MAP_18
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_19
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_25
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_16
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
```

```
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_23
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_25
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_32
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_36
  drop log
 class type inspect CSM_ZBF_CLASS_MAP_37
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_17
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_24
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_24
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_34
  drop log
 class type inspect CSM_ZBF_CLASS_MAP_35
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_14
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_27
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
```

```
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_15
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_21
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_26
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_38
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_12
 class type inspect CSM_ZBF_CLASS_MAP_15
  pass
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_21
 class type inspect CSM_ZBF_CLASS_MAP_27
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_28
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_29
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_13
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class class-default
```

```
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_20
 class type inspect CSM_ZBF_CLASS_MAP_26
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_27
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_28
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_29
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_10
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_23
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_31
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_32
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_33
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_11
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_22
 class type inspect CSM_ZBF_CLASS_MAP_30
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_9
 class type inspect CSM_ZBF_CLASS_MAP_13
  pass
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_8
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_12
  inspect Inspect-1
```

```
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_7
 class type inspect CSM_ZBF_CLASS_MAP_9
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_10
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_11
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_6
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_5
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_8
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_4
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_7
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_3
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_5
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_2
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_4
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_1
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_2
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
```

```
  drop
policy-map BRANCH-LAN-EDGE-IN
 class BRANCH-MISSION-CRITICAL
  set ip dscp 25
 class BRANCH-TRANSACTIONAL-DATA
  set ip dscp af21
 class BRANCH-NET-MGMT
  set ip dscp cs2
 class BRANCH-BULK-DATA
  set ip dscp af11
 class BRANCH-SCAVENGER
  set ip dscp cs1
!
zone security S_WAN
 description Store WAN Link
zone security S_R-2-R
 description Bridge link between routers
zone security LOOPBACK
 description Loopback interface
zone security S_MGMT
 description VLAN1000 Management
zone security S_Security
 description VLAN20 Physical Security Systems
zone security S_WAAS
 description VLAN19 WAAS optimization
zone security S_WLC-AP
 description VLAN18 Wireless Systems
zone security S_Data
 description VLAN12 Store Data
zone security S_Data-W
 description VLAN14 Store Wireless Data
zone security S_Guest
 description VLAN17 Guest/Public Wireless
zone security S_Voice
 description VLAN13 Store Voice
zone security S_Partners
 description VLAN16 Partner network
zone security S_POS
 description VLAN 11 POS Data
zone security S_POS-W
 description VLAN15 Store Wireless POS
zone security S_HIPAA
 description VLAN21 HIPAA
zone security S_HIPAA-WU
 description VLAN15 Wireless HIPAA Users
zone security S_HIPAA-WD
 description VLAN15 Wireless HIPAA Devices
zone-pair security CSM_S_WAN-LOOPBACK_1 source S_WAN destination LOOPBACK
 service-policy type inspect CSM_ZBF_POLICY_MAP_1
zone-pair security CSM_S_WAN-S_MGMT_1 source S_WAN destination S_MGMT
 service-policy type inspect CSM_ZBF_POLICY_MAP_2
zone-pair security CSM_S_WAN-S_Security_1 source S_WAN destination S_Security
 service-policy type inspect CSM_ZBF_POLICY_MAP_3
zone-pair security CSM_S_WAN-S_WAAS_1 source S_WAN destination S_WAAS
 service-policy type inspect CSM_ZBF_POLICY_MAP_4
zone-pair security CSM_S_WAN-S_WLC-AP_1 source S_WAN destination S_WLC-AP
 service-policy type inspect CSM_ZBF_POLICY_MAP_5
zone-pair security CSM_S_WAN-S_Data_1 source S_WAN destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Data-W_1 source S_WAN destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Guest_1 source S_WAN destination S_Guest
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Partners_1 source S_WAN destination S_Partners
```

```
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_POS_1 source S_WAN destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_POS-W_1 source S_WAN destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_HIPAA_1 source S_WAN destination S_HIPAA
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_HIPAA-WU_1 source S_WAN destination S_HIPAA-WU
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_Voice_1 source S_WAN destination S_Voice
 service-policy type inspect CSM_ZBF_POLICY_MAP_8
zone-pair security CSM_S_R-2-R-LOOPBACK_1 source S_R-2-R destination LOOPBACK
 service-policy type inspect CSM_ZBF_POLICY_MAP_1
zone-pair security CSM_S_R-2-R-S_MGMT_1 source S_R-2-R destination S_MGMT
 service-policy type inspect CSM_ZBF_POLICY_MAP_2
zone-pair security CSM_S_R-2-R-S_Security_1 source S_R-2-R destination S_Security
 service-policy type inspect CSM_ZBF_POLICY_MAP_3
zone-pair security CSM_S_R-2-R-S_WAAS_1 source S_R-2-R destination S_WAAS
 service-policy type inspect CSM_ZBF_POLICY_MAP_4
zone-pair security CSM_S_R-2-R-S_WLC-AP_1 source S_R-2-R destination S_WLC-AP
 service-policy type inspect CSM_ZBF_POLICY_MAP_5
zone-pair security CSM_S_R-2-R-self_1 source S_R-2-R destination self
 service-policy type inspect CSM_ZBF_POLICY_MAP_9
zone-pair security CSM_S_R-2-R-S_Data_1 source S_R-2-R destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_R-2-R-S_Data-W_1 source S_R-2-R destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_R-2-R-S_Guest_1 source S_R-2-R destination S_Guest
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_R-2-R-S_Partners_1 source S_R-2-R destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_R-2-R-S_POS_1 source S_R-2-R destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_R-2-R-S_POS-W_1 source S_R-2-R destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_R-2-R-S_HIPAA_1 source S_R-2-R destination S_HIPAA
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_R-2-R-S_HIPAA-WU _1 source S_R-2-R destination S_HIPAA-WU
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_R-2-R-S_Voice_1 source S_R-2-R destination S_Voice
 service-policy type inspect CSM_ZBF_POLICY_MAP_11
zone-pair security CSM_self-S_R-2-R_1 source self destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_12
zone-pair security CSM_LOOPBACK-S_WAN_1 source LOOPBACK destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_13
zone-pair security CSM_LOOPBACK-S_R-2-R_1 source LOOPBACK destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_13
zone-pair security CSM_LOOPBACK-S_POS_1 source LOOPBACK destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_LOOPBACK-S_POS-W_1 source LOOPBACK destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_MGMT-S_WAN_1 source S_MGMT destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_15
zone-pair security CSM_S_MGMT-S_R-2-R_1 source S_MGMT destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_15
zone-pair security CSM_S_MGMT-S_POS_1 source S_MGMT destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_MGMT-S_POS-W_1 source S_MGMT destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Security-S_WAN_1 source S_Security destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_16
zone-pair security CSM_S_Security-S_R-2-R_1 source S_Security destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_16
zone-pair security CSM_S_Security-S_POS_1 source S_Security destination S_POS
```

```
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Security-S_POS-W_1 source S_Security destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_WAN_1 source S_WAAS destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_17
zone-pair security CSM_S_WAAS-S_R-2-R_1 source S_WAAS destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_17
zone-pair security CSM_S_WAAS-S_POS_1 source S_WAAS destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_POS-W_1 source S_WAAS destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_Data_1 source S_WAAS destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
zone-pair security CSM_S_WAAS-S_Data-W_1 source S_WAAS destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
zone-pair security CSM_S_WAAS-S_Partners_1 source S_WAAS destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
zone-pair security CSM_S_WLC-AP-S_WAN_1 source S_WLC-AP destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_19
zone-pair security CSM_S_WLC-AP-S_R-2-R_1 source S_WLC-AP destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_19
zone-pair security CSM_S_WLC-AP-S_POS_1 source S_WLC-AP destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WLC-AP-S_POS-W_1 source S_WLC-AP destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_POS-S_WAN_1 source S_POS destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_20
zone-pair security CSM_S_POS-S_R-2-R_1 source S_POS destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_20
zone-pair security CSM_S_POS-W-S_WAN_1 source S_POS-W destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_21
zone-pair security CSM_S_POS-W-S_R-2-R_1 source S_POS-W destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_21
zone-pair security CSM_S_POS-W-S_POS_1 source S_POS-W destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_22
zone-pair security CSM_S_Data-S_POS_1 source S_Data destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Data-S_POS-W_1 source S_Data destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Data-S_WAN_1 source S_Data destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_23
zone-pair security CSM_S_Data-S_R-2-R_1 source S_Data destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_23
zone-pair security CSM_S_Data-W-S_POS_1 source S_Data-W destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Data-W-S_POS-W_1 source S_Data-W destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Data-W-S_WAN_1 source S_Data-W destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_23
zone-pair security CSM_S_Data-W-S_R-2-R_1 source S_Data-W destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_23
zone-pair security CSM_S_Guest-S_POS_1 source S_Guest destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Guest-S_POS-W_1 source S_Guest destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Guest-S_WAN_1 source S_Guest destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_24
zone-pair security CSM_S_Guest-S_R-2-R_1 source S_Guest destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_24
zone-pair security CSM_S_Partners-S_POS_1 source S_Partners destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Partners-S_POS-W_1 source S_Partners destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Partners-S_WAN_1 source S_Partners destination S_WAN
```

```
 service-policy type inspect CSM_ZBF_POLICY_MAP_25
zone-pair security CSM_S_Partners-S_R-2-R_1 source S_Partners destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_25
zone-pair security CSM_S_Voice-S_POS_1 source S_Voice destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Voice-S_POS-W_1 source S_Voice destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Voice-S_WAN_1 source S_Voice destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_26
zone-pair security CSM_S_Voice-S_R-2-R_1 source S_Voice destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_27
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.10.110.2 255.255.255.255
 ip pim sparse-dense-mode
 zone-member security LOOPBACK
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.102
 description ROUTER LINK TO
 encapsulation dot1Q 102
 ip address 10.10.110.30 255.255.255.252
 ip pim sparse-dense-mode
 zone-member security S_R-2-R
!
interface GigabitEthernet0/1
 description ROUTER LINK TO SWITCH
 no ip address
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/1.11
 description POS
 encapsulation dot1Q 11
 ip address 10.10.96.3 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 ip ips Store-IPS in
 ip ips Store-IPS out
 zone-member security S_POS
 standby 11 ip 10.10.96.1
 standby 11 priority 99
 standby 11 preempt
 ip igmp query-interval 125
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.12
 description DATA
 encapsulation dot1Q 12
 ip address 10.10.97.3 255.255.255.0
 ip helper-address 192.168.42.130
 ip wccp 61 redirect in
```

```
 ip pim sparse-dense-mode
 zone-member security S_Data
 standby 12 ip 10.10.97.1
 standby 12 priority 99
 standby 12 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.13
 description VOICE
 encapsulation dot1Q 13
 ip address 10.10.98.3 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_Voice
 standby 13 ip 10.10.98.1
 standby 13 priority 99
 standby 13 preempt
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.14
 description WIRELESS
 encapsulation dot1Q 14
 ip address 10.10.99.3 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Data-W
 standby 14 ip 10.10.99.1
 standby 14 priority 99
 standby 14 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.15
 description WIRELESS-POS
 encapsulation dot1Q 15
 ip address 10.10.100.3 255.255.255.0
 ip helper-address 192.168.42.130
 ip ips Store-IPS in
 ip ips Store-IPS out
 zone-member security S_POS-W
 standby 15 ip 10.10.100.1
 standby 15 priority 99
 standby 15 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.16
 description PARTNER
 encapsulation dot1Q 16
 ip address 10.10.101.3 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Partners
 standby 16 ip 10.10.101.1
 standby 16 priority 99
 standby 16 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.17
 description WIRELESS-GUEST
 encapsulation dot1Q 17
 ip address 10.10.102.3 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Guest
```

```
 standby 17 ip 10.10.102.1
 standby 17 priority 99
 standby 17 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.18
 description WIRELESS-CONTROL
 encapsulation dot1Q 18
 ip address 10.10.103.3 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_WLC-AP
 standby 18 ip 10.10.103.1
 standby 18 priority 99
 standby 18 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.19
 description WAAS
 encapsulation dot1Q 19
 ip address 10.10.104.3 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_WAAS
 standby 19 ip 10.10.104.1
 standby 19 priority 99
 standby 19 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.20
 description SECURITY-SYSTEMS
 encapsulation dot1Q 20
 ip address 10.10.105.3 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_Security
 standby 20 ip 10.10.105.1
 standby 20 priority 99
 standby 20 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.21
 description HIPAA
 encapsulation dot1Q 21
 ip address 10.10.106.3 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_HIPAA
 standby 21 ip 10.10.106.1
 standby 21 priority 99
 standby 21 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.22
 description WIRELESS-HIPAA-USERS
 encapsulation dot1Q 22
 ip address 10.10.107.3 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_HIPAA-WU
 standby 22 ip 10.10.107.1
```

```
 standby 22 priority 99
 standby 22 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.23
 description WIRELESS-HIPAA-DEVICES
 encapsulation dot1Q 23
 ip address 10.10.108.3 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_HIPAA-WD
 standby 23 ip 10.10.108.1
 standby 23 priority 99
 standby 23 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.101
 description ROUTER LINK TO
 encapsulation dot1Q 101
 ip address 10.10.110.26 255.255.255.252
 ip pim sparse-dense-mode
 zone-member security S_R-2-R
!
interface GigabitEthernet0/1.1000
 description MANAGEMENT
 encapsulation dot1Q 1000
 ip address 10.10.111.3 255.255.255.0
 zone-member security S_MGMT
 standby 100 ip 10.10.111.1
 standby 100 priority 99
 standby 100 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/2
 ip address 10.10.254.96 255.255.255.0
 ip ips Store-IPS in
 ip ips Store-IPS out
 zone-member security S_WAN
 duplex auto
 speed auto
 service-policy output BRANCH-WAN-EDGE
!
!
router ospf 5
 router-id 10.10.110.2
 redistribute connected subnets
 passive-interface default
 no passive-interface GigabitEthernet0/0.102
 no passive-interface GigabitEthernet0/1.101
 network 10.10.0.0 0.0.255.255 area 10
 default-information originate
!
no ip forward-protocol nd
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication CiscoACS
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
!
```

```
ip route 0.0.0.0 0.0.0.0 10.10.254.11
ip tacacs source-interface Loopback0
!
ip access-list extended BULK-DATA-APPS
 remark ---File Transfer---
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
 remark ---E-mail traffic---
 permit tcp any any eq smtp
 permit tcp any any eq pop3
 permit tcp any any eq 143
 remark ---other EDM app protocols---
 permit tcp any any range 3460 3466
 permit tcp any range 3460 3466 any
 remark ---messaging services---
 permit tcp any any eq 2980
 permit tcp any eq 2980 any
 remark ---Microsoft file services---
 permit tcp any any range 137 139
 permit tcp any range 137 139 any
ip access-list extended CSM_ZBF_CMAP_ACL_1
 remark Data Center Mgmt to Devices
 permit object-group CSM_INLINE_svc_rule_81604380993 object-group
CSM_INLINE_src_rule_81604380993 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_10
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381011 object-group DC-POS-Oracle
object-group BRANCH-POS
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381015 object-group DC-POS-SAP object-group
BRANCH-POS
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381019 object-group DC-POS-Tomax
object-group BRANCH-POS
ip access-list extended CSM_ZBF_CMAP_ACL_11
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381021 object-group
CSM_INLINE_src_rule_81604381021 object-group BRANCH-POS
ip access-list extended CSM_ZBF_CMAP_ACL_12
 remark Data Center VOICE (wired and Wireless)
 permit object-group CSM_INLINE_svc_rule_81604381057 object-group DC-Voice object-group
Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_13
 permit ospf object-group CSM_INLINE_src_rule_81604381150 object-group
CSM_INLINE_dst_rule_81604381150
ip access-list extended CSM_ZBF_CMAP_ACL_14
 remark Store WAAS to Clients and Servers
 permit object-group CSM_INLINE_svc_rule_81604381055 object-group Branches-ALL
object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_15
 permit ospf object-group CSM_INLINE_src_rule_81604381152 object-group
CSM_INLINE_dst_rule_81604381152
ip access-list extended CSM_ZBF_CMAP_ACL_16
 remark Syslog and SNMP Alerts
 permit object-group CSM_INLINE_svc_rule_81604380995 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_81604380995
ip access-list extended CSM_ZBF_CMAP_ACL_17
 remark Store to Data Center Authentications
 permit object-group CSM_INLINE_svc_rule_81604381001 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_81604381001
ip access-list extended CSM_ZBF_CMAP_ACL_18
 remark Store to Data Center for NTP
 permit object-group NTP object-group Branches-ALL object-group NTP-Servers
ip access-list extended CSM_ZBF_CMAP_ACL_19
```

```
 remark Store to Data Center for DHCP and DNS
 permit object-group CSM_INLINE_svc_rule_81604381035 object-group Branches-ALL
object-group ActiveDirectory.cisco-irn.com
ip access-list extended CSM_ZBF_CMAP_ACL_2
 remark Data Center subscribe to IPS SDEE events
 permit tcp object-group RSA-enVision object-group Branches-ALL eq 443
ip access-list extended CSM_ZBF_CMAP_ACL_20
 remark Permit ICMP traffic
 permit object-group CSM_INLINE_svc_rule_81604381039 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_81604381039
ip access-list extended CSM_ZBF_CMAP_ACL_21
 remark Store UCS E-series server to Data Center vShphere
 permit object-group CSM_INLINE_svc_rule_81604381005 object-group Branches-ALL
object-group vSphere-1
ip access-list extended CSM_ZBF_CMAP_ACL_22
 remark Store NAC
 permit object-group CSM_INLINE_svc_rule_81604381037 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_81604381037
ip access-list extended CSM_ZBF_CMAP_ACL_23
 remark Store to Data Center Physical Security
 permit ip object-group Branches-ALL object-group CSM_INLINE_dst_rule_81604381049
ip access-list extended CSM_ZBF_CMAP_ACL_24
 remark Store WAAS (WAAS Devices need their own zone)
 permit object-group CSM_INLINE_svc_rule_81604381053 object-group Branches-ALL
object-group DC-WAAS
ip access-list extended CSM_ZBF_CMAP_ACL_25
 remark Store to Data Center wireless controller traffic
 permit object-group CSM_INLINE_svc_rule_81604381045 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_81604381045
ip access-list extended CSM_ZBF_CMAP_ACL_26
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381009 object-group BRANCH-POS object-group
DC-POS-Oracle
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381013 object-group BRANCH-POS object-group
DC-POS-SAP
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381017 object-group BRANCH-POS object-group
DC-POS-Tomax
ip access-list extended CSM_ZBF_CMAP_ACL_27
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381023 object-group
CSM_INLINE_src_rule_81604381023 object-group BRANCH-POS
ip access-list extended CSM_ZBF_CMAP_ACL_28
 remark Store to Data Center for E-mail
 permit object-group CSM_INLINE_svc_rule_81604381025 object-group BRANCH-POS object-group
MSExchange
ip access-list extended CSM_ZBF_CMAP_ACL_29
 remark Store to Data Center for Windows Updates
 permit object-group CSM_INLINE_svc_rule_81604381027 object-group BRANCH-POS object-group
MS-Update
ip access-list extended CSM_ZBF_CMAP_ACL_3
 remark Permit ICMP traffic
 permit object-group CSM_INLINE_svc_rule_81604381041 object-group
CSM_INLINE_src_rule_81604381041 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_30
 remark Permit POS clients to talk to branch POS server
 permit object-group CSM_INLINE_svc_rule_81604381029 object-group BRANCH-POS object-group
BRANCH-POS
ip access-list extended CSM_ZBF_CMAP_ACL_31
 remark Store to Data Center for Windows Updates
 permit object-group CSM_INLINE_svc_rule_81604381061 object-group Branches-ALL
object-group MS-Update
ip access-list extended CSM_ZBF_CMAP_ACL_32
```

```
 remark Store to Data Center for E-mail
 permit object-group CSM_INLINE_svc_rule_81604381063 object-group Branches-ALL
object-group MSExchange
ip access-list extended CSM_ZBF_CMAP_ACL_33
 remark Store DATA (wired and Wireless - Access to DC Other applications)
 permit object-group CSM_INLINE_svc_rule_81604381065 object-group Branches-ALL
object-group DC-Applications
ip access-list extended CSM_ZBF_CMAP_ACL_34
 remark Store GUEST - Drop Traffic to Enterprise
 permit ip object-group Branches-ALL object-group CSM_INLINE_dst_rule_81604381071
ip access-list extended CSM_ZBF_CMAP_ACL_35
 remark Store GUEST (access to internet/DMZ web servers)
 permit ip object-group Branches-ALL any
ip access-list extended CSM_ZBF_CMAP_ACL_36
 remark Store PARTNERS - Drop Traffic to Enterprise
 permit ip object-group Branches-ALL object-group CSM_INLINE_dst_rule_81604381067
ip access-list extended CSM_ZBF_CMAP_ACL_37
 remark Store PARTNERS (wired and wireless - Access to Partner site, Internet VPN)
 permit ip object-group Branches-ALL any
ip access-list extended CSM_ZBF_CMAP_ACL_38
 remark Store VOICE (wired and Wireless - Acess to corporate wide voice)
 permit object-group CSM_INLINE_svc_rule_81604381059 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_81604381059
ip access-list extended CSM_ZBF_CMAP_ACL_4
 remark Data Center vSphere to UCS E-series server
 permit object-group CSM_INLINE_svc_rule_81604381003 object-group vSphere-1 object-group
Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_5
 remark Data Center to Store Physical Security
 permit ip object-group CSM_INLINE_src_rule_81604381047 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_6
 remark Data Center Mgmt to Devices
 permit object-group RDP object-group DC-Admin object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_7
 remark Data Center WAAS to Store
 permit object-group CSM_INLINE_svc_rule_81604381051 object-group
CSM_INLINE_src_rule_81604381051 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_8
 remark Data Center Wireless Control to AP's and Controllers in branchs
 permit object-group CSM_INLINE_svc_rule_81604381043 object-group
CSM_INLINE_src_rule_81604381043 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_9
 remark Data Center Mgmt to Devices
 permit object-group RDP object-group DC-Admin object-group BRANCH-POS
ip access-list extended MISSION-CRITICAL-SERVERS
 remark ---POS Applications---
 permit ip any 192.168.52.0 0.0.0.255
ip access-list extended NET-MGMT-APPS
 remark - Router user Authentication - Identifies TACACS Control traffic
 permit tcp any any eq tacacs
 permit tcp any eq tacacs any
ip access-list extended TRANSACTIONAL-DATA-APPS
 remark ---Workbrain Application---
 remark --Large Store Clock Server to Central Clock Application
 permit tcp host 10.10.49.94 host 192.168.46.72 eq 8444
 remark --Large branch Clock Server to CUAE
 permit tcp host 10.10.49.94 host 192.168.45.185 eq 8000
 remark ---LiteScape Application---
 permit ip any host 192.168.46.82
 permit ip any 239.192.0.0 0.0.0.255
 permit ip any host 239.255.255.250
 remark ---Remote Desktop---
 permit tcp any any eq 3389
 permit tcp any eq 3389 any
```

```
 remark ---Oracle SIM---
 permit tcp any 192.168.46.0 0.0.0.255 eq 7777
 permit tcp any 192.168.46.0 0.0.0.255 eq 6003
 permit tcp any 192.168.46.0 0.0.0.255 range 12401 12500
 permit tcp 192.168.46.0 0.0.0.255 eq 7777 any
 permit tcp 192.168.46.0 0.0.0.255 eq 6003 any
 permit tcp 192.168.46.0 0.0.0.255 range 12401 12500 any
!
logging esm config
logging trap debugging
logging source-interface Loopback0
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
!
!
!
nls resp-timeout 1
cpd cr-id 1
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps flash insertion removal
snmp-server enable traps energywise
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps ipsla
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server domain-stripping
tacacs-server key 7 <removed>
!
!
control-plane
!
!
```

```
!
!
mgcp profile default
!
!
!
!
!
gatekeeper
 shutdown
!
!
banner exec C
WARNING:
**** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
**** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner incoming C
WARNING:
**** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
**** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner login
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!

!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication CiscoACS
line aux 0
 session-timeout 1  output
 exec-timeout 0 1
 privilege level 0
 login authentication CiscoACS
 no exec
 transport preferred none
 transport output none
line vty 0 4
 session-timeout 15  output
 access-class 23 in
```

```
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162
end
```

S-A2-LRG-1

```
version 15.0
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service compress-config
service sequence-numbers
!
hostname S-A2-LRG-1
!
boot-start-marker
boot system flash bootflash:cat4500e-universalk9.SPA.03.01.00.SG.150-1.XO.bin
boot-end-marker
!
logging buffered 50000
no logging rate-limit
enable secret 5 <removed>
!

username bart privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
!
aaa new-model
!
!
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
```

```
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
ip subnet-zero
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
!
!
no ip bootp server
ip vrf Mgmt-vrf
!
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
vtp mode transparent
!
password encryption aes
!
crypto pki trustpoint CISCO_IDEVID_SUDI
 revocation-check none
 rsakeypair CISCO_IDEVID_SUDI
!
crypto pki trustpoint CISCO_IDEVID_SUDI0
 revocation-check none
!
crypto pki trustpoint TP-self-signed-145264
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-145264
 revocation-check none
 rsakeypair TP-self-signed-145264
!
!
crypto pki certificate chain CISCO_IDEVID_SUDI
 certificate 686CBFDE00000015EFB1
  <removed>
  quit
 certificate ca 6A6967B3000000000003
  <removed>
  quit
crypto pki certificate chain CISCO_IDEVID_SUDI0
 certificate ca 5FF87B282B54DC8D42A315B568C9ADFF
  <removed>
  quit
crypto pki certificate chain TP-self-signed-145264
 certificate self-signed 01
  <removed>
  quit
power redundancy-mode redundant
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
spanning-tree mode pvst
spanning-tree extend system-id
!
redundancy
 mode rpr
```

```
!
vlan internal allocation policy ascending
!
vlan 11
 name POS
!
vlan 12
 name DATA
!
vlan 13
 name VOICE
!
vlan 14
 name WIRELESS
!
vlan 15
 name WIRELESS-POS
!
vlan 16
 name PARTNER
!
vlan 17
 name WIRELESS-GUEST
!
vlan 18
 name WIRELESS-CONTROL
!
vlan 19
 name WAAS
!
vlan 20
 name SECURITY-SYSTEMS
!
vlan 21
 name HIPAA
!
vlan 22
 name WIRELESS-HIPAA-USERS
!
vlan 23
 name WIRELESS-HIPAA-DEVICES
!
vlan 101
 name RouterLink101
!
vlan 102
 name RouterLink102
!
vlan 1000
 name MANAGEMENT
!
ip ssh version 2
ip scp server enable
!
!
interface FastEthernet1
 ip vrf forwarding Mgmt-vrf
 no ip address
 shutdown
 speed auto
 duplex auto
!
interface TenGigabitEthernet3/1
 shutdown
```

```
!
interface TenGigabitEthernet3/2
 shutdown
!
interface TenGigabitEthernet3/3
 shutdown
!
interface TenGigabitEthernet3/4
 shutdown
!
interface GigabitEthernet5/1
 shutdown
!
interface GigabitEthernet5/2
 shutdown
!
interface GigabitEthernet5/3
 shutdown
!
interface GigabitEthernet5/4
 shutdown
!
interface GigabitEthernet5/5
 shutdown
!
interface GigabitEthernet5/6
 shutdown
!
interface GigabitEthernet5/7
 shutdown
!
interface GigabitEthernet5/8
 shutdown
!
interface GigabitEthernet5/9
 shutdown
!
interface GigabitEthernet5/10
 shutdown
!
interface GigabitEthernet5/11
 shutdown
!
interface GigabitEthernet5/12
 shutdown
!
interface GigabitEthernet5/13
 shutdown
!
interface GigabitEthernet5/14
 shutdown
!
interface GigabitEthernet5/15
 shutdown
!
interface GigabitEthernet5/16
 shutdown
!
interface GigabitEthernet5/17
 shutdown
!
interface GigabitEthernet5/18
 shutdown
!
```

```
interface GigabitEthernet5/19
 shutdown
!
interface GigabitEthernet5/20
 shutdown
!
interface GigabitEthernet5/21
 shutdown
!
interface GigabitEthernet5/22
 shutdown
!
interface GigabitEthernet5/23
 shutdown
!
interface GigabitEthernet5/24
 shutdown
!
interface GigabitEthernet5/25
 shutdown
!
interface GigabitEthernet5/26
 shutdown
!
interface GigabitEthernet5/27
 shutdown
!
interface GigabitEthernet5/28
 shutdown
!
interface GigabitEthernet5/29
 shutdown
!
interface GigabitEthernet5/30
 shutdown
!
interface GigabitEthernet5/31
 shutdown
!
interface GigabitEthernet5/32
 shutdown
!
interface GigabitEthernet5/33
 shutdown
!
interface GigabitEthernet5/34
 shutdown
!
interface GigabitEthernet5/35
 shutdown
!
interface GigabitEthernet5/36
 shutdown
!
interface GigabitEthernet5/37
 shutdown
!
interface GigabitEthernet5/38
 shutdown
!
interface GigabitEthernet5/39
 shutdown
!
interface GigabitEthernet5/40
```

```
 shutdown
!
interface GigabitEthernet5/41
 shutdown
!
interface GigabitEthernet5/42
 shutdown
!
interface GigabitEthernet5/43
 shutdown
!
interface GigabitEthernet5/44
 shutdown
!
interface GigabitEthernet5/45
 shutdown
!
interface GigabitEthernet5/46
 shutdown
!
interface GigabitEthernet5/47
 shutdown
!
interface GigabitEthernet5/48
 shutdown
!
interface GigabitEthernet6/1
!
interface GigabitEthernet6/2
 shutdown
!
interface GigabitEthernet6/3
 shutdown
!
interface GigabitEthernet6/4
 shutdown
!
interface GigabitEthernet6/5
 shutdown
!
interface GigabitEthernet6/6
 shutdown
!
interface GigabitEthernet6/7
 shutdown
!
interface GigabitEthernet6/8
 shutdown
!
interface GigabitEthernet6/9
 shutdown
!
interface GigabitEthernet6/10
 description MSP-A2-LRG-1
 switchport access vlan 20
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet6/11
 shutdown
!
interface GigabitEthernet6/12
 shutdown
!
```

```
interface GigabitEthernet6/13
 shutdown
!
interface GigabitEthernet6/14
 shutdown
!
interface GigabitEthernet6/15
 shutdown
!
interface GigabitEthernet6/16
 shutdown
!
interface GigabitEthernet6/17
 description WLC-A2-LRG-1_G1
 switchport access vlan 18
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet6/18
 description WLC-A2-LRG-1_G2
 switchport trunk allowed vlan 14-17
 switchport mode trunk
!
interface GigabitEthernet6/19
 shutdown
!
interface GigabitEthernet6/20
 shutdown
!
interface GigabitEthernet6/21
 shutdown
!
interface GigabitEthernet6/22
 shutdown
!
interface GigabitEthernet6/23
 shutdown
!
interface GigabitEthernet6/24
 shutdown
!
interface GigabitEthernet6/25
 shutdown
!
interface GigabitEthernet6/26
 shutdown
!
interface GigabitEthernet6/27
 shutdown
!
interface GigabitEthernet6/28
 shutdown
!
interface GigabitEthernet6/29
 shutdown
!
interface GigabitEthernet6/30
 shutdown
!
interface GigabitEthernet6/31
 shutdown
!
interface GigabitEthernet6/32
 shutdown
```

```
!
interface GigabitEthernet6/33
 shutdown
!
interface GigabitEthernet6/34
 shutdown
!
interface GigabitEthernet6/35
 shutdown
!
interface GigabitEthernet6/36
 shutdown
!
interface GigabitEthernet6/37
 shutdown
!
interface GigabitEthernet6/38
 shutdown
!
interface GigabitEthernet6/39
 shutdown
!
interface GigabitEthernet6/40
 shutdown
!
interface GigabitEthernet6/41
 switchport mode trunk
!
interface GigabitEthernet6/42
 shutdown
!
interface GigabitEthernet6/43
 switchport mode trunk
!
interface GigabitEthernet6/44
 shutdown
!
interface GigabitEthernet6/45
 switchport mode trunk
!
interface GigabitEthernet6/46
!
interface GigabitEthernet6/47
 switchport mode trunk
!
interface GigabitEthernet6/48
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan1000
 description Management VLAN for Switch
 ip address 10.10.111.11 255.255.255.0
!
no ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 10.10.111.1
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication CiscoACS
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
```

```
ip tacacs source-interface Vlan1000
!
!
logging trap debugging
logging source-interface Vlan1000
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
snmp-server trap-source Vlan1000
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
no snmp-server enable traps license
snmp-server enable traps entity
snmp-server enable traps flash insertion removal
snmp-server enable traps power-ethernet police
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps port-security
snmp-server enable traps energywise
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps errdisable
snmp-server enable traps vlan-membership
snmp-server enable traps mac-notification change move threshold
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
banner exec ^CC
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
```

```
^C
banner incoming ^CC
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^CC
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication CiscoACS
 stopbits 1
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
!
ntp clock-period 17202862
ntp source Vlan1000
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end

S-A2-LRG-1#
```

S-A2-LRG-2

```
version 15.0
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service compress-config
```

```
service sequence-numbers
!
hostname S-A2-LRG-2
!
boot-start-marker
boot system flash bootflash:cat4500e-universalk9.SPA.03.01.00.SG.150-1.XO.bin
boot-end-marker
!
logging buffered 50000
no logging rate-limit
enable secret 5 <removed>
!

username bart privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
!
aaa new-model
!
!
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
ip subnet-zero
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
!
!
no ip bootp server
ip vrf Mgmt-vrf
!
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
vtp mode transparent
!
password encryption aes
!
crypto pki trustpoint CISCO_IDEVID_SUDI
 revocation-check none
 rsakeypair CISCO_IDEVID_SUDI
!
crypto pki trustpoint CISCO_IDEVID_SUDI0
 revocation-check none
!
crypto pki trustpoint TP-self-signed-145261
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-145261
 revocation-check none
 rsakeypair TP-self-signed-145261
!
!
```

```
crypto pki certificate chain CISCO_IDEVID_SUDI
 certificate 6B46CD9B00000015F50E
  <removed>
  quit
 certificate ca 6A6967B3000000000003
  <removed>
  quit
crypto pki certificate chain CISCO_IDEVID_SUDI0
 certificate ca 5FF87B282B54DC8D42A315B568C9ADFF
  <removed>
  quit
crypto pki certificate chain TP-self-signed-145261
 certificate self-signed 01
  <removed>
  quit
power redundancy-mode redundant
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
spanning-tree mode pvst
spanning-tree extend system-id
!
redundancy
 mode rpr
!
vlan internal allocation policy ascending
!
vlan 11
 name POS
!
vlan 12
 name DATA
!
vlan 13
 name VOICE
!
vlan 14
 name WIRELESS
!
vlan 15
 name WIRELESS-POS
!
vlan 16
 name PARTNER
!
vlan 17
 name WIRELESS-GUEST
!
vlan 18
 name WIRELESS-CONTROL
!
vlan 19
 name WAAS
!
vlan 20
 name SECURITY-SYSTEMS
!
vlan 21
 name HIPAA
```

```
!
vlan 22
 name WIRELESS-HIPAA-USERS
!
vlan 23
 name WIRELESS-HIPAA-DEVICES
!
vlan 101
 name RouterLink101
!
vlan 102
 name RouterLink102
!
vlan 1000
 name MANAGEMENT
!
ip ssh version 2
ip scp server enable
!
!
interface FastEthernet1
 ip vrf forwarding Mgmt-vrf
 no ip address
 shutdown
 speed auto
 duplex auto
!
interface TenGigabitEthernet3/1
 shutdown
!
interface TenGigabitEthernet3/2
 shutdown
!
interface TenGigabitEthernet3/3
 shutdown
!
interface TenGigabitEthernet3/4
 shutdown
!
interface GigabitEthernet6/1
!
interface GigabitEthernet6/2
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/3
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/4
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/5
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/6
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/7
 switchport access vlan 17
 shutdown
```

```
!
interface GigabitEthernet6/8
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/9
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/10
 description MSP-A2-LRG-1
 switchport access vlan 20
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet6/11
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/12
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/13
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/14
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/15
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/16
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/17
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/18
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/19
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/20
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/21
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/22
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/23
```

```
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/24
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/25
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/26
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/27
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/28
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/29
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/30
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/31
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/32
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/33
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/34
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/35
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/36
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/37
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/38
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/39
```

```
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/40
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet6/41
 switchport mode trunk
!
interface GigabitEthernet6/42
!
interface GigabitEthernet6/43
 switchport mode trunk
!
interface GigabitEthernet6/44
!
interface GigabitEthernet6/45
 switchport mode trunk
!
interface GigabitEthernet6/46
!
interface GigabitEthernet6/47
 switchport mode trunk
!
interface GigabitEthernet6/48
!
interface Vlan1
 no ip address
!
interface Vlan1000
 description Management VLAN for Switch
 ip address 10.10.111.12 255.255.255.0
!
no ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 10.10.111.1
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication CiscoACS
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Vlan1000
!
!
logging trap debugging
logging source-interface Vlan1000
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
```

```
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
snmp-server trap-source Vlan1000
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
no snmp-server enable traps license
snmp-server enable traps entity
snmp-server enable traps flash insertion removal
snmp-server enable traps power-ethernet police
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps port-security
snmp-server enable traps energywise
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps errdisable
snmp-server enable traps vlan-membership
snmp-server enable traps mac-notification change move threshold
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
banner exec ^CC
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^CC
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^CC
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
```

```
 login authentication CiscoACS
 stopbits 1
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
!
ntp clock-period 17211501
ntp source Vlan1000
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end
```

S-A2-LRG-3

```
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
!
hostname S-A2-LRG-3
!
boot-start-marker
boot-end-marker
!
logging buffered 50000
logging monitor informational
enable secret 5 <removed>
!

username bart privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
macro name dot1x
switchport access vlan 11
 switchport mode access
 switchport voice vlan 13
 ip arp inspection limit rate 1000
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab webauth
```

```
 authentication priority dot1x mab
 authentication port-control auto
 authentication timer reauthenticate server
 authentication timer inactivity server
 authentication violation restrict
 authentication fallback ise
 mab
 snmp trap mac-notification change added
 dot1x pae authenticator
 dot1x timeout tx-period 5
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip dhcp snooping limit rate 200
@
!
macro global description dot1x
macro auto sticky
aaa new-model
!
!
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authentication dot1x default group radius local
aaa authorization exec default group tacacs+ if-authenticated
aaa authorization network default group radius
aaa authorization auth-proxy default group radius
aaa authorization configuration default group radius
aaa accounting update newinfo
aaa accounting auth-proxy default start-stop group radius
aaa accounting dot1x default start-stop group radius
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
aaa server radius dynamic-author
 client 192.168.42.111
 server-key 7 <removed>
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
system mtu routing 1500
authentication mac-move permit
!
!
ip dhcp snooping vlan 1,11
no ip dhcp snooping information option
ip dhcp snooping
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
ip device tracking
ip admission name ise proxy http inactivity-time 60
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
vtp mode transparent
!
cts sxp enable
cts sxp default source-ip 10.10.111.13
password encryption aes
!
crypto pki trustpoint TP-self-signed-4268543232
```

```
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-4268543232
 revocation-check none
 rsakeypair TP-self-signed-4268543232
!
!
crypto pki certificate chain TP-self-signed-4268543232
 certificate self-signed 01
  <removed>
  quit
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
dot1x system-auth-control
!
fallback profile ise
 ip access-group ACL-DEFAULT in
 ip admission ise
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
vlan 11
 name POS
!
vlan 12
 name DATA
!
vlan 13
 name VOICE
!
vlan 14
 name WIRELESS
!
vlan 15
 name WIRELESS-POS
!
vlan 16
 name PARTNER
!
vlan 17
 name WIRELESS-GUEST
!
vlan 18
 name WIRELESS-CONTROL
!
vlan 19
 name WAAS
!
vlan 20
 name SECURITY-SYSTEMS
!
vlan 21
 name HIPAA
!
vlan 22
 name WIRELESS-HIPAA-USERS
```

```
!
vlan 23
 name WIRELESS-HIPAA-DEVICES
!
vlan 101
 name RouterLink101
!
vlan 102
 name RouterLink102
!
vlan 1000
 name MANAGEMENT
!
ip ssh version 2
ip scp server enable
!
!
interface FastEthernet0
 no ip address
 shutdown
!
interface GigabitEthernet0/1
 description uplink
!
interface GigabitEthernet0/2
 description uplink
!
interface GigabitEthernet0/3
 shutdown
!
interface GigabitEthernet0/4
 description Cisco9971 IP phone
 switchport access vlan 11
 switchport voice vlan 13
 spanning-tree portfast
!
interface GigabitEthernet0/5
 description IP Camera - 4300
 switchport access vlan 20
 switchport mode access
!
interface GigabitEthernet0/6
 description CIAC-GW
 switchport access vlan 20
 switchport mode access
!
interface GigabitEthernet0/7
 shutdown
!
interface GigabitEthernet0/8
 shutdown
!
interface GigabitEthernet0/9
 shutdown
!
interface GigabitEthernet0/10
 shutdown
!
interface GigabitEthernet0/11
 shutdown
!
interface GigabitEthernet0/12
 shutdown
!
```

```
interface GigabitEthernet0/13
 shutdown
!
interface GigabitEthernet0/14
 shutdown
!
interface GigabitEthernet0/15
 shutdown
!
interface GigabitEthernet0/16
 shutdown
!
interface GigabitEthernet0/17
 shutdown
!
interface GigabitEthernet0/18
 shutdown
!
interface GigabitEthernet0/19
 shutdown
!
interface GigabitEthernet0/20
 shutdown
!
interface GigabitEthernet0/21
 shutdown
!
interface GigabitEthernet0/22
 shutdown
!
interface GigabitEthernet0/23
 shutdown
!
interface GigabitEthernet0/24
 shutdown
!
interface GigabitEthernet0/25
 description open-mode 802.1x+mab+mda+acl
 switchport access vlan 11
 switchport mode access
 switchport voice vlan 13
 ip arp inspection limit rate 1000
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab webauth
 authentication priority dot1x mab
 authentication port-control auto
 authentication timer reauthenticate server
 authentication timer inactivity server
 authentication violation restrict
 authentication fallback ise
 mab
 snmp trap mac-notification change added
 dot1x pae authenticator
 dot1x timeout tx-period 5
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip dhcp snooping limit rate 200
!
interface GigabitEthernet0/26
 description mobile worker
 switchport access vlan 11
```

```
 switchport mode access
 switchport voice vlan 13
 ip arp inspection limit rate 1000
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab webauth
 authentication priority dot1x mab
 authentication port-control auto
 authentication timer reauthenticate server
 authentication timer inactivity server
 authentication violation restrict
 authentication fallback ise
 mab
 snmp trap mac-notification change added
 macro description dot1x
 dot1x pae authenticator
 dot1x timeout tx-period 5
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip dhcp snooping limit rate 200
!
interface GigabitEthernet0/27
 shutdown
!
interface GigabitEthernet0/28
 shutdown
!
interface GigabitEthernet0/29
 shutdown
!
interface GigabitEthernet0/30
 switchport access vlan 11
 switchport mode access
 switchport voice vlan 13
 ip arp inspection limit rate 1000
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab webauth
 authentication priority dot1x mab
 authentication port-control auto
 authentication timer reauthenticate server
 authentication timer inactivity server
 authentication violation restrict
 authentication fallback ise
 mab
 snmp trap mac-notification change added
 macro description dot1x
 dot1x pae authenticator
 dot1x timeout tx-period 5
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip dhcp snooping limit rate 200
!
interface GigabitEthernet0/31
 switchport access vlan 11
 switchport mode access
 switchport voice vlan 13
 ip arp inspection limit rate 1000
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
```

```
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab webauth
 authentication priority dot1x mab
 authentication port-control auto
 authentication timer reauthenticate server
 authentication timer inactivity server
 authentication violation restrict
 authentication fallback ise
 mab
 snmp trap mac-notification change added
 macro description dot1x
 dot1x pae authenticator
 dot1x timeout tx-period 5
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip dhcp snooping limit rate 200
!
interface GigabitEthernet0/32
 switchport access vlan 11
 switchport mode access
 switchport voice vlan 13
 ip arp inspection limit rate 1000
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab webauth
 authentication priority dot1x mab
 authentication port-control auto
 authentication timer reauthenticate server
 authentication timer inactivity server
 authentication violation restrict
 authentication fallback ise
 mab
 snmp trap mac-notification change added
 macro description dot1x
 dot1x pae authenticator
 dot1x timeout tx-period 5
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip dhcp snooping limit rate 200
!
interface GigabitEthernet0/33
 switchport access vlan 11
 switchport mode access
 switchport voice vlan 13
 ip arp inspection limit rate 1000
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab webauth
 authentication priority dot1x mab
 authentication port-control auto
 authentication timer reauthenticate server
 authentication timer inactivity server
 authentication violation restrict
 authentication fallback ise
 mab
 snmp trap mac-notification change added
 macro description dot1x
 dot1x pae authenticator
 dot1x timeout tx-period 5
```

```
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip dhcp snooping limit rate 200
!
interface GigabitEthernet0/34
 switchport access vlan 11
 switchport mode access
 switchport voice vlan 13
 ip arp inspection limit rate 1000
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab webauth
 authentication priority dot1x mab
 authentication port-control auto
 authentication timer reauthenticate server
 authentication timer inactivity server
 authentication violation restrict
 authentication fallback ise
 mab
 snmp trap mac-notification change added
 macro description dot1x
 dot1x pae authenticator
 dot1x timeout tx-period 5
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip dhcp snooping limit rate 200
!
interface GigabitEthernet0/35
 switchport access vlan 11
 switchport mode access
 switchport voice vlan 13
 ip arp inspection limit rate 1000
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab webauth
 authentication priority dot1x mab
 authentication port-control auto
 authentication timer reauthenticate server
 authentication timer inactivity server
 authentication violation restrict
 authentication fallback ise
 mab
 snmp trap mac-notification change added
 macro description dot1x
 dot1x pae authenticator
 dot1x timeout tx-period 5
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip dhcp snooping limit rate 200
!
interface GigabitEthernet0/36
 switchport access vlan 11
 switchport mode access
 switchport voice vlan 13
 ip arp inspection limit rate 1000
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab webauth
```

```
 authentication priority dot1x mab
 authentication port-control auto
 authentication timer reauthenticate server
 authentication timer inactivity server
 authentication violation restrict
 authentication fallback ise
 mab
 snmp trap mac-notification change added
 macro description dot1x
 dot1x pae authenticator
 dot1x timeout tx-period 5
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip dhcp snooping limit rate 200
!
interface GigabitEthernet0/37
 shutdown
!
interface GigabitEthernet0/38
 shutdown
!
interface GigabitEthernet0/39
 shutdown
!
interface GigabitEthernet0/40
 shutdown
!
interface GigabitEthernet0/41
 shutdown
!
interface GigabitEthernet0/42
 shutdown
!
interface GigabitEthernet0/43
 shutdown
!
interface GigabitEthernet0/44
 shutdown
!
interface GigabitEthernet0/45
 shutdown
!
interface GigabitEthernet0/46
 shutdown
!
interface GigabitEthernet0/47
 shutdown
!
interface GigabitEthernet0/48
 shutdown
!
interface GigabitEthernet1/1
 shutdown
!
interface GigabitEthernet1/2
 shutdown
!
interface GigabitEthernet1/3
 shutdown
!
interface GigabitEthernet1/4
 shutdown
!
interface TenGigabitEthernet1/1
```

```
 shutdown
!
interface TenGigabitEthernet1/2
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan1000
 description Management VLAN for Switch
 ip address 10.10.111.13 255.255.255.0
!
ip default-gateway 10.10.111.1
ip classless
no ip forward-protocol nd
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication CiscoACS
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Vlan1000
!
ip access-list extended ACL-ALLOW
 permit ip any any
ip access-list extended ACL-DEFAULT
 remark DHCP
 permit udp any eq bootpc any eq bootps
 remark DNS
 permit udp any any eq domain
 remark ICMP Ping
 permit icmp any any
 remark PXE Boot
 permit udp any any eq tftp
 remark URL Redirect
 permit tcp any host 192.168.42.111 eq www
 permit tcp any host 192.168.42.111 eq 443
 permit tcp any host 192.168.42.112 eq www
 permit tcp any host 192.168.42.112 eq 443
 remark Guest Portal
 permit tcp any host 192.168.42.111 eq 8443
 permit tcp any host 192.168.42.112 eq 8443
 deny   ip any any
ip access-list extended ACL-POSTURE-REDIRECT
 deny   ip any host 192.168.42.111
 deny   ip any host 192.168.42.130
 permit ip any any
ip access-list extended ACL-WEBAUTH-REDIRECT
 remark Don't match traffic sent to ISE PDP Nodes
 deny   ip any host 192.168.42.111
 deny   ip any host 192.168.42.112
 deny   ip any host 10.35.48.242
 deny   ip any host 171.71.169.207
 permit ip any any
!
ip sla enable reaction-alerts
logging trap debugging
logging origin-id ip
logging source-interface Vlan1000
logging 192.168.42.124
logging host 192.168.42.111 transport udp port 20514
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
```

```
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
snmp-server trap-source Vlan1000
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps energywise
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps power-ethernet group 1
snmp-server enable traps power-ethernet police
snmp-server enable traps cpu threshold
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps errdisable
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server host 192.168.42.124 remoteuser
snmp-server host 192.168.42.111 version 2c COMPLIANCElabISE  dot1x mac-notification snmp
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server dead-criteria time 5 tries 3
radius-server host 192.168.42.111 auth-port 1812 acct-port 1813 key 7 <removed>
radius-server vsa send accounting
radius-server vsa send authentication
!
banner exec ^CC
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
```

```
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^CC
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^CC
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication CiscoACS
 stopbits 1
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
!
ntp clock-period 36027134
ntp source Vlan1000
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
mac address-table notification change interval 0
mac address-table notification change
end
```

S-A2-LRG-4

```
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
```

```
service password-encryption
service sequence-numbers
!
hostname S-A2-LRG-4
!
boot-start-marker
boot-end-marker
!
logging buffered 50000
enable secret 5 <removed>
!

username bart privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
!
macro auto device media-player ACCESS_VLAN=12
macro auto device ip-camera ACCESS_VLAN=20
macro auto device phone ACCESS_VLAN=17 VOICE_VLAN=13
macro auto device access-point ACCESS_VLAN=18
macro auto device lightweight-ap ACCESS_VLAN=18
!
macro auto global processing fallback cdp
aaa new-model
!
!
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authentication dot1x default group radius local
aaa authorization exec default group tacacs+ if-authenticated
aaa authorization network default group radius
aaa authorization auth-proxy default group radius
aaa accounting update newinfo
aaa accounting dot1x default start-stop group radius
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
system mtu routing 1500
authentication mac-move permit
ip subnet-zero
no ip source-route
!
!
ip domain-name cisco-irn.com
ip host nac-2 192.168.42.112
ip name-server 192.168.42.130
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
mls qos map policed-dscp  24 26 46 to 0
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue input bandwidth 90 10
mls qos srr-queue input threshold 1 8 16
mls qos srr-queue input threshold 2 34 66
mls qos srr-queue input buffers 67 33
```

```
mls qos srr-queue input cos-map queue 1 threshold 2 1
mls qos srr-queue input cos-map queue 1 threshold 3 0
mls qos srr-queue input cos-map queue 2 threshold 1 2
mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7
mls qos srr-queue input cos-map queue 2 threshold 3 3 5
mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15
mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7
mls qos srr-queue input dscp-map queue 1 threshold 3 32
mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23
mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 48
mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56
mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47
mls qos srr-queue output cos-map queue 1 threshold 3 5
mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 2 4
mls qos srr-queue output cos-map queue 4 threshold 2 1
mls qos srr-queue output cos-map queue 4 threshold 3 0
mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47
mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39
mls qos srr-queue output dscp-map queue 4 threshold 1 8
mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15
mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7
mls qos queue-set output 1 threshold 1 138 138 92 138
mls qos queue-set output 1 threshold 2 138 138 92 400
mls qos queue-set output 1 threshold 3 36 77 100 318
mls qos queue-set output 1 threshold 4 20 50 67 400
mls qos queue-set output 2 threshold 1 149 149 100 149
mls qos queue-set output 2 threshold 2 118 118 100 235
mls qos queue-set output 2 threshold 3 41 68 100 272
mls qos queue-set output 2 threshold 4 42 72 100 242
mls qos queue-set output 1 buffers 10 10 26 54
mls qos queue-set output 2 buffers 16 6 17 61
mls qos
password encryption aes
!
crypto pki trustpoint TP-self-signed-4268542976
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-4268542976
 revocation-check none
 rsakeypair TP-self-signed-4268542976
!
!
crypto pki certificate chain TP-self-signed-4268542976
 certificate self-signed 01
  <removed> 1
  quit
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
dot1x system-auth-control
spanning-tree mode pvst
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
!
!
!
```

```
!
vlan internal allocation policy ascending
!
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh version 2
ip scp server enable
!
class-map match-all AutoQoS-VoIP-RTP-Trust
 match ip dscp ef
class-map match-all AutoQoS-VoIP-Control-Trust
 match ip dscp cs3  af31
!
!
policy-map AutoQoS-Police-CiscoPhone
 class AutoQoS-VoIP-RTP-Trust
  set dscp ef
  police 320000 8000 exceed-action policed-dscp-transmit
 class AutoQoS-VoIP-Control-Trust
  set dscp cs3
  police 32000 8000 exceed-action policed-dscp-transmit
!
!
!
interface FastEthernet0
 no ip address
 shutdown
!
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 srr-queue bandwidth share 10 10 60 20
 queue-set 2
 priority-queue out
 mls qos trust cos
 macro description CISCO_SWITCH_EVENT
 auto qos voip trust
!
interface GigabitEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 srr-queue bandwidth share 10 10 60 20
 queue-set 2
 priority-queue out
 mls qos trust cos
 macro description CISCO_SWITCH_EVENT
 auto qos voip trust
!
interface GigabitEthernet0/3
 description AIR-CAP3502E
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 18
 switchport trunk allowed vlan 14-18
 switchport mode access
 switchport block unicast
 switchport port-security aging time 1
 switchport port-security violation protect
 switchport port-security aging type inactivity
 load-interval 30
 srr-queue bandwidth share 10 10 60 20
 priority-queue out
 mls qos trust dscp
 macro description CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT
 storm-control broadcast level pps 1k
```

```
 storm-control multicast level pps 2k
 storm-control action trap
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip dhcp snooping limit rate 15
!
interface GigabitEthernet0/4
 description AIR-CAP3502I
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 18
 switchport trunk allowed vlan 14-18
 switchport mode access
 switchport block unicast
 switchport port-security aging time 1
 switchport port-security violation protect
 switchport port-security aging type inactivity
 load-interval 30
 srr-queue bandwidth share 10 10 60 20
 priority-queue out
 mls qos trust dscp
 macro description CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT
 storm-control broadcast level pps 1k
 storm-control multicast level pps 2k
 storm-control action trap
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip dhcp snooping limit rate 15
!
interface GigabitEthernet0/5
 shutdown
!
interface GigabitEthernet0/6
 shutdown
!
interface GigabitEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
 srr-queue bandwidth share 10 10 60 20
 queue-set 2
 priority-queue out
 mls qos trust cos
 macro description CISCO_SWITCH_EVENT
 auto qos voip trust
!
interface GigabitEthernet0/8
 shutdown
!
interface GigabitEthernet0/9
 shutdown
!
interface GigabitEthernet0/10
 shutdown
!
interface GigabitEthernet0/11
 description Cisco7975 IP phone
 switchport mode access
 switchport block unicast
 switchport voice vlan 2
 switchport port-security maximum 3
 switchport port-security maximum 2 vlan access
 switchport port-security
 switchport port-security aging time 1
 switchport port-security violation restrict
 switchport port-security aging type inactivity
```

```
 load-interval 30
 srr-queue bandwidth share 10 10 60 20
 queue-set 2
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 macro description CISCO_PHONE_EVENT
 auto qos voip cisco-phone
 storm-control broadcast level pps 1k
 storm-control multicast level pps 2k
 storm-control action trap
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input AutoQoS-Police-CiscoPhone
 ip dhcp snooping limit rate 15
!
interface GigabitEthernet0/12
 shutdown
!
interface GigabitEthernet0/13
 shutdown
!
interface GigabitEthernet0/14
 shutdown
!
interface GigabitEthernet0/15
 shutdown
!
interface GigabitEthernet0/16
 shutdown
!
interface GigabitEthernet0/17
 shutdown
!
interface GigabitEthernet0/18
 shutdown
!
interface GigabitEthernet0/19
 shutdown
!
interface GigabitEthernet0/20
 shutdown
!
interface GigabitEthernet0/21
 shutdown
!
interface GigabitEthernet0/22
 shutdown
!
interface GigabitEthernet0/23
 shutdown
!
interface GigabitEthernet0/24
 shutdown
!
interface GigabitEthernet0/25
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
```

```
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/26
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/27
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/28
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/29
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/30
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
```

```
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/31
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/32
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/33
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/34
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
```

```
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/35
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/36
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/37
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/38
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/39
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
```

```
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/40
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/41
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/42
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/43
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
```

```
!
interface GigabitEthernet0/44
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/45
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/46
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/47
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet0/48
 description open-mode 802.1x+mab+mda+acl
 switchport mode access
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-domain
```

```
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 spanning-tree portfast
!
interface GigabitEthernet1/1
 shutdown
!
interface GigabitEthernet1/2
 shutdown
!
interface GigabitEthernet1/3
 shutdown
!
interface GigabitEthernet1/4
 shutdown
!
interface TenGigabitEthernet1/1
 shutdown
!
interface TenGigabitEthernet1/2
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan1000
 description Management VLAN for Switch
 ip address 10.10.111.14 255.255.255.0
!
ip default-gateway 10.10.111.1
ip classless
no ip forward-protocol nd
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication CiscoACS
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Vlan1000
!
ip access-list extended ACL-DEFAULT
 remark DHCP
 permit udp any eq bootpc any eq bootps
 remark DNS
 permit udp any any eq domain
 remark ICMP Ping
 permit icmp any any
 remark PXE Boot
 permit udp any any eq tftp
 remark URL Redirect
 permit tcp any host 192.168.42.111 eq www
 permit tcp any host 192.168.42.111 eq 443
 permit tcp any host 192.168.42.112 eq www
 permit tcp any host 192.168.42.112 eq 443
 remark Guest Portal
 permit tcp any host 192.168.42.111 eq 8443
 permit tcp any host 192.168.42.112 eq 8443
 deny   ip any any
ip access-list extended ACL-WEBAUTH-REDIRECT
 remark Don't match traffic sent to ISE PDP Nodes
```

```
 deny   ip any host 192.168.42.111
 deny   ip any host 192.168.42.112
 deny   ip any host 10.35.48.242
 remark Don't match traffic sent to remediation services (wwwin-download.cisco.com)
 deny   ip any host 171.71.169.207
 remark Match all other traffic for redirection
 permit ip any any
!
ip sla enable reaction-alerts
logging trap debugging
logging source-interface Vlan1000
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFF0F
snmp-server trap-source Vlan1000
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps energywise
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps power-ethernet group 1
snmp-server enable traps power-ethernet police
snmp-server enable traps cpu threshold
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps errdisable
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server host 192.168.42.124 remoteuser
snmp-server host 192.168.42.111 version 2c COMPLIANCElabISE  dot1x mac-notification snmp
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
radius-server dead-criteria time 5 tries 3
radius-server host 192.168.42.111 auth-port 1812 acct-port 1813 key 7 <removed>
!
```

```
banner exec ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication CiscoACS
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
!
ntp clock-period 36027569
ntp source Vlan1000
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end
```

S-A2-LRG-5

```
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
!
hostname S-A2-LRG-5
!
boot-start-marker
boot-end-marker
!
shell trigger POS-Systems POS-Systems
logging buffered 51200
enable secret 5 <removed>
!

username bart privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
!
macro global description cisco-desktop
macro auto execute CISCO_LAST_RESORT_EVENT builtin CISCO_AP_AUTO_SMARTPORT ACCESS_VLAN=17
macro auto execute COMPLIANCE-POS builtin CISCO_PHONE_AUTO_SMARTPORT ACCESS_VLAN=11
VOICE_VLAN=13
macro auto execute POS-Systems remote scp://SMARTPORT@192.168.42.122/POS-Systems.txt
ACCESS_VLAN=11 VOICE_VLAN=13
!
macro auto mac-address-group COMPLIANCE-POS
 oui list 001C26
 oui list 001C25
 mac-address list 0021.5C02.1DEF
 mac-address list 001C.25BE.99C2
macro auto device media-player ACCESS_VLAN=12
macro auto device ip-camera ACCESS_VLAN=20
macro auto device phone ACCESS_VLAN=17 VOICE_VLAN=13
macro auto device access-point ACCESS_VLAN=18
macro auto device lightweight-ap ACCESS_VLAN=18
!
macro auto global processing fallback cdp
aaa new-model
!
!
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
system mtu routing 1500
!
```

```
!
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
mls qos srr-queue output cos-map queue 2 threshold 1 2
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40 41 42 43 44 45
mls qos srr-queue output dscp-map queue 1 threshold 3 46 47
mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28 29 30 31 34 35
mls qos srr-queue output dscp-map queue 2 threshold 1 36 37 38 39
mls qos srr-queue output dscp-map queue 2 threshold 2 24
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3 4 5 6 7
mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11 13 15
mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
mls qos queue-set output 1 threshold 1 100 100 50 200
mls qos queue-set output 1 threshold 2 125 125 100 400
mls qos queue-set output 1 threshold 3 100 100 100 400
mls qos queue-set output 1 threshold 4 60 150 50 200
mls qos queue-set output 1 buffers 15 25 40 20
mls qos
password encryption aes
!
crypto pki trustpoint TP-self-signed-3964801920
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3964801920
 revocation-check none
 rsakeypair TP-self-signed-3964801920
!
!
crypto pki certificate chain TP-self-signed-3964801920
 certificate self-signed 01
  <removed>
  quit
spanning-tree mode pvst
spanning-tree extend system-id
auto qos srnd4
!
!
!
!
vlan internal allocation policy ascending
!
ip ssh version 2
ip scp server enable
!
!
interface GigabitEthernet0/1
 switchport access vlan 17
!
interface GigabitEthernet0/2
 switchport access vlan 17
!
```

```
interface GigabitEthernet0/3
 switchport access vlan 17
!
interface GigabitEthernet0/4
 switchport access vlan 17
!
interface GigabitEthernet0/5
 switchport access vlan 17
!
interface GigabitEthernet0/6
 switchport access vlan 17
!
interface GigabitEthernet0/7
 switchport access vlan 17
!
interface GigabitEthernet0/8
 switchport access vlan 17
!
interface GigabitEthernet0/9
 description Uplink to S-A2-LRG-4 G0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
 srr-queue bandwidth share 1 30 35 5
 queue-set 2
 priority-queue out
 mls qos trust cos
 macro description CISCO_SWITCH_EVENT
 auto qos trust
!
interface GigabitEthernet0/10
!
interface Vlan1
 no ip address
!
interface Vlan1000
 description Management VLAN for Switch
 ip address 10.10.111.15 255.255.255.0
!
ip default-gateway 10.10.111.1
ip classless
no ip forward-protocol nd
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication CiscoACS
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Vlan1000
!
!
ip sla enable reaction-alerts
logging trap debugging
logging source-interface Vlan1000
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
```

```
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
snmp-server trap-source Vlan1000
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps energywise
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131 timeout 5
tacacs-server directed-request
tacacs-server key 7 <removed>
!
banner exec ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication CiscoACS
 speed 115200
line vty 0 4
 session-timeout 15  output
 access-class 23 in
```

```
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
!
ntp clock-period 22518292
ntp source Vlan1000
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
!
end
```

Medium Clinic

R-A2-MED-1

```
version 15.1
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
!
hostname R-A2-Med-1
!
boot-start-marker
boot system flash0 c2951-universalk9-mz.SPA.151-3.T.bin
boot-end-marker
!
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 50000
no logging rate-limit
enable secret 5 <removed>
!
aaa new-model
!
!
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default
 action-type start-stop
 group tacacs+
```

```
!
aaa accounting commands 15 default
 action-type start-stop
 group tacacs+
!
aaa accounting system default
 action-type start-stop
 group tacacs+
!
!
!
!
!
!
aaa session-id common
!
memory-size iomem 25
clock timezone PST -8 0
clock summer-time PSTDST recurring
!
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-1670063162
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1670063162
 revocation-check none
 rsakeypair TP-self-signed-1670063162
!
!
crypto pki certificate chain TP-self-signed-1670063162
 certificate self-signed 01
  <removed>
    quit
no ipv6 cef
no ip source-route
ip cef
!
!
!
ip multicast-routing
!
!
no ip bootp server
ip domain name cisco-irn.com
ip name-server 192.168.42.130
ip inspect audit-trail
ip ips config location ipstest retries 1 timeout 1
ip ips notify SDEE
ip ips name COMPLIANCE-XXX
!
ip ips signature-category
  category all
   retired true
  category ios_ips basic
   retired false
!
ip wccp 61
ip wccp 62
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
multilink bundle-name authenticated
```

```
!
parameter-map type inspect global
 WAAS enable
parameter-map type inspect Inspect-1
 audit-trail on

parameter-map type trend-global trend-glob-map
!
!
!
!
password encryption aes
voice-card 0
!
!
!
!
!
!
!
license udi pid STARSCREAM sn <removed>
hw-module pvdm 0/2
!
hw-module sm 1
!
hw-module sm 2
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
object-group network ActiveDirectory.cisco-irn.com
 host 192.168.42.130
!
object-group service CAPWAP
 description CAPWAP UDP ports 5246 and 5247
 udp eq 5246
 udp eq 5247
!
object-group service CISCO-WAAS
 description Ports for Cisco WAAS
 tcp eq 4050
!
object-group network EMC-NCM
 description EMC Network Configuration Manager
 host 192.168.42.122
!
object-group network RSA-enVision
 description RSA EnVision Syslog collector and SIM
 host 192.168.42.124
!
object-group network CSM_INLINE_dst_rule_81604380995
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object EMC-NCM
 group-object RSA-enVision
!
object-group network TACACS
 description Csico Secure ACS server for TACACS and Radius
 host 192.168.42.131
!
object-group network RSA-AM
```

```
 description RSA Authentication Manager for SecureID
 host 192.168.42.137
!
object-group network NAC-1
 description ISE server for NAC
 host 192.168.42.111
!
object-group network CSM_INLINE_dst_rule_81604381001
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object ActiveDirectory.cisco-irn.com
 group-object TACACS
 group-object RSA-AM
 group-object NAC-1
!
object-group network NAC-2
 host 192.168.42.112
!
object-group network CSM_INLINE_dst_rule_81604381037
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object NAC-2
 group-object NAC-1
!
object-group network DC-ALL
 description All of the Data Center
 192.168.0.0 255.255.0.0
!
object-group network Branches-ALL
 description all branch networks
 10.10.0.0 255.255.0.0
!
object-group network CSM_INLINE_dst_rule_81604381039
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
!
object-group network WCSManager
 description Wireless Manager
 host 192.168.43.135
!
object-group network DC-Wifi-Controllers
 description Central Wireless Controllers for branchs
 host 192.168.43.21
 host 192.168.43.22
!
object-group network DC-Wifi-MSE
 description Mobility Service Engines
 host 192.168.43.31
 host 192.168.43.32
!
object-group network CSM_INLINE_dst_rule_81604381045
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
!
object-group network PAME-DC-1
 host 192.168.44.111
!
object-group network MSP-DC-1
 description Data Center VSOM
 host 192.168.44.121
!
object-group network CSM_INLINE_dst_rule_81604381049
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
```

```
 group-object PAME-DC-1
 group-object MSP-DC-1
!
object-group network CSM_INLINE_dst_rule_81604381059
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
!
object-group network CSM_INLINE_dst_rule_81604381067
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
!
object-group network CSM_INLINE_dst_rule_81604381071
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
!
object-group network CSM_INLINE_dst_rule_81604381150
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 10.10.126.0 255.255.255.0
 10.10.110.0 255.255.255.0
!
object-group network CSM_INLINE_dst_rule_81604381152
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 10.10.126.0 255.255.255.0
 10.10.110.0 255.255.255.0
!
object-group network DC-Admin
 description DC Admin Systems
 host 192.168.41.101
 host 192.168.41.102
!
object-group network CSManager
 description Cisco Security Manager
 host 192.168.42.133
!
object-group network CSM_INLINE_src_rule_81604380993
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-Admin
 group-object EMC-NCM
 group-object CSManager
!
object-group network DC-POS-Tomax
 description Tomax POS Communication from Store to Data Center
 192.168.52.96 255.255.255.224
!
object-group network DC-POS-SAP
 description SAP POS Communication from Store to Data Center
 192.168.52.144 255.255.255.240
!
object-group network DC-POS-Oracle
 description Oracle POS Communication from Store to Data Center
 192.168.52.128 255.255.255.240
!
object-group network CSM_INLINE_src_rule_81604381021
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-Admin
 group-object DC-POS-Tomax
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
!
object-group network CSM_INLINE_src_rule_81604381023
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
```

```
 group-object DC-Admin
 group-object DC-POS-Tomax
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
!
object-group network CSM_INLINE_src_rule_81604381041
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
!
object-group network CSM_INLINE_src_rule_81604381043
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
!
object-group network CSM_INLINE_src_rule_81604381047
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object PAME-DC-1
 group-object MSP-DC-1
!
object-group network DC-WAAS
 description WAE Appliances in Data Center
 host 192.168.48.10
 host 192.168.49.10
 host 192.168.47.11
 host 192.168.47.12
!
object-group network CSM_INLINE_src_rule_81604381051
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-Admin
 group-object DC-WAAS
!
object-group network CSM_INLINE_src_rule_81604381150
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 10.10.126.0 255.255.255.0
 10.10.110.0 255.255.255.0
!
object-group network CSM_INLINE_src_rule_81604381152
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 10.10.126.0 255.255.255.0
 10.10.110.0 255.255.255.0
!
object-group service CSM_INLINE_svc_rule_81604380993
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
!
object-group service CSM_INLINE_svc_rule_81604380995
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 udp eq syslog
 udp eq snmp
 udp eq snmptrap
!
object-group service CSM_INLINE_svc_rule_81604381001
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq tacacs
 udp eq 1812
 udp eq 1813
 tcp eq 389
 tcp eq 636
```

```
!
object-group service vCenter-to-ESX4
 description Communication from vCetner to ESX hosts
 tcp eq 5989
 tcp eq 8000
 tcp eq 902
 tcp eq 903
!
object-group service CSM_INLINE_svc_rule_81604381003
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq 22
 group-object vCenter-to-ESX4
!
object-group service ESX-SLP
 description CIM Service Location Protocol (SLP) for VMware systems
 udp eq 427
 tcp eq 427
!
object-group service CSM_INLINE_svc_rule_81604381005
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 group-object vCenter-to-ESX4
 group-object ESX-SLP
!
object-group service ORACLE-RMI
 description RMI TCP ports 1300 and 1301-1319.
 tcp range 1300 1319
!
object-group service ORACLE-Weblogic
 description HTTP/RMI and HTTPS/RMI-SSL 7001 & 7002. OracleAQ uses 1521.
 tcp eq 7001
 tcp eq 7002
 tcp eq 1521
!
object-group service ORACLE-WAS
 description RMI/IIOP over 2809  HTTP over 9443 IBM-MQ 1414
 tcp eq 2809
 tcp eq 9443
 tcp eq 1414
!
object-group service ORACLE-OAS
 description OAS uses one port for HTTP and RMI - 12601.
 tcp eq 12601
!
object-group service CSM_INLINE_svc_rule_81604381009
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
 group-object ORACLE-RMI
 group-object ORACLE-Weblogic
 group-object ORACLE-WAS
 group-object ORACLE-OAS
!
object-group service CSM_INLINE_svc_rule_81604381011
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
 group-object ORACLE-RMI
```

```
 group-object ORACLE-Weblogic
 group-object ORACLE-WAS
 group-object ORACLE-OAS
!
object-group service HTTPS-8443
 tcp eq 8443
!
object-group service CSM_INLINE_svc_rule_81604381013
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
 group-object HTTPS-8443
!
object-group service CSM_INLINE_svc_rule_81604381015
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
 group-object HTTPS-8443
!
object-group service TOMAX-8990
 description Tomax Application Port
 tcp eq 8990
!
object-group service CSM_INLINE_svc_rule_81604381017
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 group-object TOMAX-8990
!
object-group service CSM_INLINE_svc_rule_81604381019
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 group-object TOMAX-8990
!
object-group service ICMP-Requests
 description ICMP requests
 icmp information-request
 icmp mask-request
 icmp timestamp-request
!
object-group service CSM_INLINE_svc_rule_81604381021
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
 icmp redirect
 icmp alternate-address
 group-object ICMP-Requests
!
object-group service CSM_INLINE_svc_rule_81604381023
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
 icmp redirect
 icmp alternate-address
 group-object ICMP-Requests
```

```
!
object-group service CSM_INLINE_svc_rule_81604381025
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq smtp
 tcp eq pop3
 tcp eq 143
!
object-group service CSM_INLINE_svc_rule_81604381027
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_81604381029
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp
 udp
 tcp eq 443
!
object-group service DNS-Resolving
 description Domain Name Server
 tcp eq domain
 udp eq domain
!
object-group service CSM_INLINE_svc_rule_81604381035
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 udp eq bootps
 group-object DNS-Resolving
!
object-group service CSM_INLINE_svc_rule_81604381037
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
 group-object HTTPS-8443
!
object-group service CSM_INLINE_svc_rule_81604381039
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
!
object-group service CSM_INLINE_svc_rule_81604381041
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
!
object-group service LWAPP
 description LWAPP UDP ports 12222 and 12223
 udp eq 12222
 udp eq 12223
!
object-group service TFTP
 description Trivial File Transfer
```

```
 tcp eq 69
 udp eq tftp
!
object-group service IP-Protocol-97
 description IP protocol 97
 97
!
object-group service CSM_INLINE_svc_rule_81604381043
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq www
 tcp eq 22
 tcp eq telnet
 udp eq isakmp
 group-object CAPWAP
 group-object LWAPP
 group-object TFTP
 group-object IP-Protocol-97
!
object-group service Cisco-Mobility
 description Mobility ports for Wireless
 udp eq 16666
 udp eq 16667
!
object-group service CSM_INLINE_svc_rule_81604381045
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 udp eq isakmp
 group-object CAPWAP
 group-object LWAPP
 group-object Cisco-Mobility
 group-object IP-Protocol-97
!
object-group service Microsoft-DS-SMB
 description Microsoft-DS Active Directory, Windows shares Microsoft-DS SMB file sharing
 tcp eq 445
!
object-group service CSM_INLINE_svc_rule_81604381051
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp
 tcp eq 139
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_81604381053
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp
 tcp eq 139
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_81604381055
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp
 tcp eq 139
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_81604381057
```

```
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp
 tcp-udp eq 5060
 tcp eq 2000
 tcp eq www
 tcp eq 443
 group-object TFTP
!
object-group service CSM_INLINE_svc_rule_81604381059
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp-udp eq 5060
 tcp eq 2000
!
object-group service CSM_INLINE_svc_rule_81604381061
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_81604381063
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq smtp
 tcp eq pop3
 tcp eq 143
!
object-group service Netbios
 description Netbios Servers
 udp eq netbios-dgm
 udp eq netbios-ns
 tcp eq 139
!
object-group service ORACLE-SIM
 description Oracle Store Inventory Management
 tcp eq 7777
 tcp eq 6003
 tcp range 12401 12500
!
object-group service RDP
 description Windows Remote Desktop
 tcp eq 3389
!
object-group service Workbrain
 tcp eq 8444
!
object-group service CSM_INLINE_svc_rule_81604381065
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq ftp
 tcp eq www
 tcp eq 443
 udp eq 88
 tcp-udp eq 42
 group-object Microsoft-DS-SMB
 group-object Netbios
 group-object ORACLE-SIM
 group-object RDP
 group-object Workbrain
!
object-group network DC-Applications
```

```
 description Applications in the Data Center
 192.168.180.0 255.255.254.0
!
object-group network DC-Voice
 description Data Center Voice
 192.168.45.0 255.255.255.0
!
object-group network MS-Update
 description Windows Update Server
 host 192.168.42.150
!
object-group network MSExchange
 description Mail Server
 host 192.168.42.140
!
object-group service NTP
 description NTP Protocols
 tcp eq 123
 udp eq ntp
!
object-group network NTP-Servers
 description NTP Servers
 host 192.168.62.161
 host 162.168.62.162
!
object-group network BRANCH-POS
 10.10.0.0 255.255.0.0
!
object-group network vSphere-1
 description vSphere server for Lab
 host 192.168.41.102
!

username bart privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
!
redundancy
!
!
!
!
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh version 2
ip scp server enable
!
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_7
 match protocol http
 match protocol https
 match protocol microsoft-ds
 match protocol ms-sql
 match protocol ms-sql-m
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol oracle
 match protocol oracle-em-vp
 match protocol oraclenames
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_10
 match access-group name CSM_ZBF_CMAP_ACL_10
 match class-map CSM_ZBF_CMAP_PLMAP_7
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_4
```

```
 match protocol http
 match protocol https
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_23
 match access-group name CSM_ZBF_CMAP_ACL_23
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_17
 match protocol http
 match protocol https
 match protocol imap3
 match protocol pop3
 match protocol pop3s
 match protocol smtp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_32
 match access-group name CSM_ZBF_CMAP_ACL_32
 match class-map CSM_ZBF_CMAP_PLMAP_17
class-map type inspect match-all CSM_ZBF_CLASS_MAP_11
 match access-group name CSM_ZBF_CMAP_ACL_11
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_14
 match protocol http
 match protocol https
class-map type inspect match-all CSM_ZBF_CLASS_MAP_22
 match access-group name CSM_ZBF_CMAP_ACL_22
 match class-map CSM_ZBF_CMAP_PLMAP_14
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_20
 match protocol http
 match protocol https
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
 match protocol ftp
 match protocol ssh
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_33
 match access-group name CSM_ZBF_CMAP_ACL_33
 match class-map CSM_ZBF_CMAP_PLMAP_20
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_8
 match protocol sip
 match protocol sip-tls
 match protocol skinny
 match protocol tftp
 match protocol http
 match protocol https
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_12
 match access-group name CSM_ZBF_CMAP_ACL_12
 match class-map CSM_ZBF_CMAP_PLMAP_8
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_13
 match protocol https
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_21
 match access-group name CSM_ZBF_CMAP_ACL_21
 match class-map CSM_ZBF_CMAP_PLMAP_13
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_19
 match protocol http
 match protocol https
 match protocol icmp
 match protocol tcp
 match protocol udp
```

```
class-map type inspect match-all CSM_ZBF_CLASS_MAP_30
 match access-group name CSM_ZBF_CMAP_ACL_30
 match class-map CSM_ZBF_CMAP_PLMAP_19
class-map type inspect match-all CSM_ZBF_CLASS_MAP_13
 match access-group name CSM_ZBF_CMAP_ACL_13
class-map type inspect match-all CSM_ZBF_CLASS_MAP_20
 match access-group name CSM_ZBF_CMAP_ACL_20
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_18
 match protocol http
 match protocol https
 match protocol udp
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_31
 match access-group name CSM_ZBF_CMAP_ACL_31
 match class-map CSM_ZBF_CMAP_PLMAP_18
class-map match-all BRANCH-BULK-DATA
 match protocol tftp
 match protocol nfs
 match access-group name BULK-DATA-APPS
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_5
 match protocol http
 match protocol https
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_14
 match access-group name CSM_ZBF_CMAP_ACL_14
 match class-map CSM_ZBF_CMAP_PLMAP_5
class-map type inspect match-all CSM_ZBF_CLASS_MAP_27
 match access-group name CSM_ZBF_CMAP_ACL_27
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_36
 match access-group name CSM_ZBF_CMAP_ACL_36
class-map type inspect match-all CSM_ZBF_CLASS_MAP_15
 match access-group name CSM_ZBF_CMAP_ACL_15
class-map type inspect match-all CSM_ZBF_CLASS_MAP_26
 match access-group name CSM_ZBF_CMAP_ACL_26
 match class-map CSM_ZBF_CMAP_PLMAP_7
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_21
 match protocol tcp
 match protocol udp
 match protocol http
 match protocol https
class-map type inspect match-all CSM_ZBF_CLASS_MAP_37
 match access-group name CSM_ZBF_CMAP_ACL_37
 match class-map CSM_ZBF_CMAP_PLMAP_21
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_9
 match protocol syslog
 match protocol syslog-conn
 match protocol snmp
 match protocol snmptrap
class-map type inspect match-all CSM_ZBF_CLASS_MAP_16
 match access-group name CSM_ZBF_CMAP_ACL_16
 match class-map CSM_ZBF_CMAP_PLMAP_9
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_16
 match protocol http
 match protocol https
 match protocol isakmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_25
```

```
 match access-group name CSM_ZBF_CMAP_ACL_25
 match class-map CSM_ZBF_CMAP_PLMAP_16
class-map type inspect match-all CSM_ZBF_CLASS_MAP_34
 match access-group name CSM_ZBF_CMAP_ACL_34
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_10
 match protocol ldaps
 match protocol ldap
 match protocol ldap-admin
 match protocol radius
 match protocol tacacs
 match protocol tacacs-ds
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_17
 match access-group name CSM_ZBF_CMAP_ACL_17
 match class-map CSM_ZBF_CMAP_PLMAP_10
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_15
 match protocol http
 match protocol https
 match protocol netbios-ns
 match protocol netbios-dgm
 match protocol netbios-ssn
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_24
 match access-group name CSM_ZBF_CMAP_ACL_24
 match class-map CSM_ZBF_CMAP_PLMAP_15
class-map type inspect match-all CSM_ZBF_CLASS_MAP_35
 match access-group name CSM_ZBF_CMAP_ACL_35
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_11
 match protocol ntp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_18
 match access-group name CSM_ZBF_CMAP_ACL_18
 match class-map CSM_ZBF_CMAP_PLMAP_11
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_12
 match protocol bootpc
 match protocol bootps
 match protocol udp
 match protocol tcp
 match protocol dns
 match protocol dhcp-failover
class-map type inspect match-all CSM_ZBF_CLASS_MAP_19
 match access-group name CSM_ZBF_CMAP_ACL_19
 match class-map CSM_ZBF_CMAP_PLMAP_12
class-map type inspect match-all CSM_ZBF_CLASS_MAP_29
 match access-group name CSM_ZBF_CMAP_ACL_29
 match class-map CSM_ZBF_CMAP_PLMAP_18
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_22
 match protocol sip
 match protocol sip-tls
 match protocol skinny
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_38
 match access-group name CSM_ZBF_CMAP_ACL_38
 match class-map CSM_ZBF_CMAP_PLMAP_22
class-map type inspect match-all CSM_ZBF_CLASS_MAP_28
 match access-group name CSM_ZBF_CMAP_ACL_28
 match class-map CSM_ZBF_CMAP_PLMAP_17
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_1
 match protocol https
 match protocol ssh
```

```
class-map type inspect match-all CSM_ZBF_CLASS_MAP_1
 match access-group name CSM_ZBF_CMAP_ACL_1
 match class-map CSM_ZBF_CMAP_PLMAP_1
class-map type inspect match-all CSM_ZBF_CLASS_MAP_3
 match access-group name CSM_ZBF_CMAP_ACL_3
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_2
 match protocol https
 match protocol http
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_2
 match access-group name CSM_ZBF_CMAP_ACL_2
 match class-map CSM_ZBF_CMAP_PLMAP_2
class-map type inspect match-all CSM_ZBF_CLASS_MAP_5
 match access-group name CSM_ZBF_CMAP_ACL_5
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_3
 match protocol http
 match protocol https
 match protocol ssh
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_4
 match access-group name CSM_ZBF_CMAP_ACL_4
 match class-map CSM_ZBF_CMAP_PLMAP_3
class-map type inspect match-all CSM_ZBF_CLASS_MAP_7
 match access-group name CSM_ZBF_CMAP_ACL_7
 match class-map CSM_ZBF_CMAP_PLMAP_5
class-map type inspect match-all CSM_ZBF_CLASS_MAP_6
 match access-group name CSM_ZBF_CMAP_ACL_6
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_9
 match access-group name CSM_ZBF_CMAP_ACL_9
 match protocol tcp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_6
 match protocol http
 match protocol https
 match protocol ssh
 match protocol telnet
 match protocol tftp
 match protocol isakmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_8
 match access-group name CSM_ZBF_CMAP_ACL_8
 match class-map CSM_ZBF_CMAP_PLMAP_6
class-map match-all BULK-DATA
 match ip dscp af11  af12
class-map match-all INTERACTIVE-VIDEO
 match ip dscp af41  af42
class-map match-any BRANCH-TRANSACTIONAL-DATA
 match protocol citrix
 match protocol ldap
 match protocol telnet
 match protocol sqlnet
 match protocol http url "*SalesReport*"
 match access-group name TRANSACTIONAL-DATA-APPS
class-map match-all BRANCH-MISSION-CRITICAL
 match access-group name MISSION-CRITICAL-SERVERS
class-map match-all VOICE
 match ip dscp ef
class-map match-all MISSION-CRITICAL-DATA
 match ip dscp 25
class-map match-any BRANCH-NET-MGMT
```

```
 match protocol snmp
 match protocol syslog
 match protocol dns
 match protocol icmp
 match protocol ssh
 match access-group name NET-MGMT-APPS
class-map match-all ROUTING
 match ip dscp cs6
class-map match-all SCAVENGER
 match ip dscp cs1
class-map match-all NET-MGMT
 match ip dscp cs2
class-map match-any BRANCH-SCAVENGER
 match protocol gnutella
 match protocol fasttrack
 match protocol kazaa2
class-map match-any CALL-SIGNALING
 match ip dscp cs3
class-map match-all TRANSACTIONAL-DATA
 match ip dscp af21  af22
!
!
policy-map BRANCH-LAN-EDGE-OUT
 class class-default
policy-map BRANCH-WAN-EDGE
 class VOICE
  priority percent 18
 class INTERACTIVE-VIDEO
  priority percent 15
 class CALL-SIGNALING
  bandwidth percent 5
 class ROUTING
  bandwidth percent 3
 class NET-MGMT
  bandwidth percent 2
 class MISSION-CRITICAL-DATA
  bandwidth percent 15
  random-detect
 class TRANSACTIONAL-DATA
  bandwidth percent 12
  random-detect dscp-based
 class BULK-DATA
  bandwidth percent 4
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 1
 class class-default
  bandwidth percent 25
  random-detect
policy-map type inspect CSM_ZBF_POLICY_MAP_18
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_19
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
```

```
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_25
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_16
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_23
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_25
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_32
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_36
  drop log
 class type inspect CSM_ZBF_CLASS_MAP_37
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_17
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_24
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_24
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_34
```

```
  drop log
 class type inspect CSM_ZBF_CLASS_MAP_35
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_14
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_27
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_15
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_21
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_26
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_38
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_12
 class type inspect CSM_ZBF_CLASS_MAP_15
  pass
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_21
 class type inspect CSM_ZBF_CLASS_MAP_27
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_28
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_29
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
```

```
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_13
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_20
 class type inspect CSM_ZBF_CLASS_MAP_26
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_27
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_28
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_29
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_10
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_23
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_31
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_32
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_33
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_11
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
```

```
policy-map type inspect CSM_ZBF_POLICY_MAP_22
 class type inspect CSM_ZBF_CLASS_MAP_30
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_9
 class type inspect CSM_ZBF_CLASS_MAP_13
  pass
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_8
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_12
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_7
 class type inspect CSM_ZBF_CLASS_MAP_9
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_10
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_11
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_6
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_5
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_8
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_4
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_7
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_3
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_5
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_2
 class type inspect CSM_ZBF_CLASS_MAP_1
```

```
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_4
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_1
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_2
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop
policy-map BRANCH-LAN-EDGE-IN
 class BRANCH-MISSION-CRITICAL
  set ip dscp 25
 class BRANCH-TRANSACTIONAL-DATA
  set ip dscp af21
 class BRANCH-NET-MGMT
  set ip dscp cs2
 class BRANCH-BULK-DATA
  set ip dscp af11
 class BRANCH-SCAVENGER
  set ip dscp cs1
!
zone security S_WAN
 description Store WAN Link
zone security S_R-2-R
 description Bridge link between routers
zone security LOOPBACK
 description Loopback interface
zone security S_MGMT
 description VLAN1000 Management
zone security S_Security
 description VLAN20 Physical Security Systems
zone security S_WAAS
 description VLAN19 WAAS optimization
zone security S_WLC-AP
 description VLAN18 Wireless Systems
zone security S_Data
 description VLAN12 Store Data
zone security S_Data-W
 description VLAN14 Store Wireless Data
zone security S_Guest
 description VLAN17 Guest/Public Wireless
zone security S_Voice
 description VLAN13 Store Voice
zone security S_Partners
 description VLAN16 Partner network
zone security S_POS
 description VLAN 11 POS Data
zone security S_POS-W
 description VLAN15 Store Wireless POS
zone security S_HIPAA
 description VLAN21 HIPAA
zone security S_HIPAA-WU
 description VLAN15 Wireless HIPAA Users
zone security S_HIPAA-WD
 description VLAN15 Wireless HIPAA Devices
zone-pair security CSM_S_WAN-LOOPBACK_1 source S_WAN destination LOOPBACK
 service-policy type inspect CSM_ZBF_POLICY_MAP_1
```

```
zone-pair security CSM_S_WAN-S_MGMT_1 source S_WAN destination S_MGMT
 service-policy type inspect CSM_ZBF_POLICY_MAP_2
zone-pair security CSM_S_WAN-S_Security_1 source S_WAN destination S_Security
 service-policy type inspect CSM_ZBF_POLICY_MAP_3
zone-pair security CSM_S_WAN-S_WAAS_1 source S_WAN destination S_WAAS
 service-policy type inspect CSM_ZBF_POLICY_MAP_4
zone-pair security CSM_S_WAN-S_WLC-AP_1 source S_WAN destination S_WLC-AP
 service-policy type inspect CSM_ZBF_POLICY_MAP_5
zone-pair security CSM_S_WAN-S_Data_1 source S_WAN destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Data-W_1 source S_WAN destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Guest_1 source S_WAN destination S_Guest
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Partners_1 source S_WAN destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_POS_1 source S_WAN destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_POS-W_1 source S_WAN destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_HIPAA_1 source S_WAN destination S_HIPAA
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_HIPAA-WU_1 source S_WAN destination S_HIPAA-WU
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_Voice_1 source S_WAN destination S_Voice
 service-policy type inspect CSM_ZBF_POLICY_MAP_8
zone-pair security CSM_S_R-2-R-LOOPBACK_1 source S_R-2-R destination LOOPBACK
 service-policy type inspect CSM_ZBF_POLICY_MAP_1
zone-pair security CSM_S_R-2-R-S_MGMT_1 source S_R-2-R destination S_MGMT
 service-policy type inspect CSM_ZBF_POLICY_MAP_2
zone-pair security CSM_S_R-2-R-S_Security_1 source S_R-2-R destination S_Security
 service-policy type inspect CSM_ZBF_POLICY_MAP_3
zone-pair security CSM_S_R-2-R-S_WAAS_1 source S_R-2-R destination S_WAAS
 service-policy type inspect CSM_ZBF_POLICY_MAP_4
zone-pair security CSM_S_R-2-R-S_WLC-AP_1 source S_R-2-R destination S_WLC-AP
 service-policy type inspect CSM_ZBF_POLICY_MAP_5
zone-pair security CSM_S_R-2-R-self_1 source S_R-2-R destination self
 service-policy type inspect CSM_ZBF_POLICY_MAP_9
zone-pair security CSM_S_R-2-R-S_Data_1 source S_R-2-R destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_R-2-R-S_Data-W_1 source S_R-2-R destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_R-2-R-S_Guest_1 source S_R-2-R destination S_Guest
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_R-2-R-S_Partners_1 source S_R-2-R destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_R-2-R-S_POS_1 source S_R-2-R destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_R-2-R-S_POS-W_1 source S_R-2-R destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_R-2-R-S_HIPAA_1 source S_R-2-R destination S_HIPAA
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_R-2-R-S_HIPAA-WU _1 source S_R-2-R destination S_HIPAA-WU
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_R-2-R-S_Voice_1 source S_R-2-R destination S_Voice
 service-policy type inspect CSM_ZBF_POLICY_MAP_11
zone-pair security CSM_self-S_R-2-R_1 source self destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_12
zone-pair security CSM_LOOPBACK-S_WAN_1 source LOOPBACK destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_13
zone-pair security CSM_LOOPBACK-S_R-2-R_1 source LOOPBACK destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_13
zone-pair security CSM_LOOPBACK-S_POS_1 source LOOPBACK destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
```

```
zone-pair security CSM_LOOPBACK-S_POS-W_1 source LOOPBACK destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_MGMT-S_WAN_1 source S_MGMT destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_15
zone-pair security CSM_S_MGMT-S_R-2-R_1 source S_MGMT destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_15
zone-pair security CSM_S_MGMT-S_POS_1 source S_MGMT destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_MGMT-S_POS-W_1 source S_MGMT destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Security-S_WAN_1 source S_Security destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_16
zone-pair security CSM_S_Security-S_R-2-R_1 source S_Security destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_16
zone-pair security CSM_S_Security-S_POS_1 source S_Security destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Security-S_POS-W_1 source S_Security destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_WAN_1 source S_WAAS destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_17
zone-pair security CSM_S_WAAS-S_R-2-R_1 source S_WAAS destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_17
zone-pair security CSM_S_WAAS-S_POS_1 source S_WAAS destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_POS-W_1 source S_WAAS destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_Data_1 source S_WAAS destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
zone-pair security CSM_S_WAAS-S_Data-W_1 source S_WAAS destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
zone-pair security CSM_S_WAAS-S_Partners_1 source S_WAAS destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
zone-pair security CSM_S_WLC-AP-S_WAN_1 source S_WLC-AP destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_19
zone-pair security CSM_S_WLC-AP-S_R-2-R_1 source S_WLC-AP destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_19
zone-pair security CSM_S_WLC-AP-S_POS_1 source S_WLC-AP destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WLC-AP-S_POS-W_1 source S_WLC-AP destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_POS-S_WAN_1 source S_POS destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_20
zone-pair security CSM_S_POS-S_R-2-R_1 source S_POS destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_20
zone-pair security CSM_S_POS-W-S_WAN_1 source S_POS-W destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_21
zone-pair security CSM_S_POS-W-S_R-2-R_1 source S_POS-W destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_21
zone-pair security CSM_S_POS-W-S_POS_1 source S_POS-W destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_22
zone-pair security CSM_S_Data-S_POS_1 source S_Data destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Data-S_POS-W_1 source S_Data destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Data-S_WAN_1 source S_Data destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_23
zone-pair security CSM_S_Data-S_R-2-R_1 source S_Data destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_23
zone-pair security CSM_S_Data-W-S_POS_1 source S_Data-W destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Data-W-S_POS-W_1 source S_Data-W destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Data-W-S_WAN_1 source S_Data-W destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_23
```

```
zone-pair security CSM_S_Data-W-S_R-2-R_1 source S_Data-W destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_23
zone-pair security CSM_S_Guest-S_POS_1 source S_Guest destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Guest-S_POS-W_1 source S_Guest destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Guest-S_WAN_1 source S_Guest destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_24
zone-pair security CSM_S_Guest-S_R-2-R_1 source S_Guest destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_24
zone-pair security CSM_S_Partners-S_POS_1 source S_Partners destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Partners-S_POS-W_1 source S_Partners destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Partners-S_WAN_1 source S_Partners destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_25
zone-pair security CSM_S_Partners-S_R-2-R_1 source S_Partners destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_25
zone-pair security CSM_S_Voice-S_POS_1 source S_Voice destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Voice-S_POS-W_1 source S_Voice destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Voice-S_WAN_1 source S_Voice destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_26
zone-pair security CSM_S_Voice-S_R-2-R_1 source S_Voice destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_27
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.10.126.1 255.255.255.255
 ip pim sparse-dense-mode
 zone-member security LOOPBACK
!
interface GigabitEthernet0/0
 ip address 10.10.255.112 255.255.255.0
 ip ips COMPLIANCE-XXX in
 zone-member security S_WAN
 duplex auto
 speed auto
 service-policy output BRANCH-WAN-EDGE
!
interface GigabitEthernet0/1
 description ROUTER LINK TO SWITCH
 no ip address
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/1.11
 description POS
 encapsulation dot1Q 11
 ip address 10.10.112.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_POS
 standby 11 ip 10.10.112.1
 standby 11 priority 101
 standby 11 preempt
 ip igmp query-interval 125
```

```
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.12
 description DATA
 encapsulation dot1Q 12
 ip address 10.10.113.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip wccp 61 redirect in
 ip pim sparse-dense-mode
 zone-member security S_Data
 standby 12 ip 10.10.113.1
 standby 12 priority 101
 standby 12 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.13
 description VOICE
 encapsulation dot1Q 13
 ip address 10.10.114.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_Voice
 standby 13 ip 10.10.114.1
 standby 13 priority 101
 standby 13 preempt
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.14
 description WIRELESS
 encapsulation dot1Q 14
 ip address 10.10.115.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Data-W
 standby 14 ip 10.10.115.1
 standby 14 priority 101
 standby 14 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.15
 description WIRELESS-POS
 encapsulation dot1Q 15
 ip address 10.10.116.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_POS-W
 standby 15 ip 10.10.116.1
 standby 15 priority 101
 standby 15 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.16
 description PARTNER
 encapsulation dot1Q 16
 ip address 10.10.117.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Partners
 standby 16 ip 10.10.117.1
 standby 16 priority 101
 standby 16 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
```

```
!
interface GigabitEthernet0/1.17
 description WIRELESS-GUEST
 encapsulation dot1Q 17
 ip address 10.10.118.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Guest
 standby 17 ip 10.10.118.1
 standby 17 priority 101
 standby 17 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.18
 description WIRELESS-CONTROL
 encapsulation dot1Q 18
 ip address 10.10.119.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_WLC-AP
 standby 18 ip 10.10.119.1
 standby 18 priority 101
 standby 18 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.19
 description WAAS
 encapsulation dot1Q 19
 ip address 10.10.120.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_WAAS
 standby 19 ip 10.10.120.1
 standby 19 priority 101
 standby 19 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.20
 description SECURITY-SYSTEMS
 encapsulation dot1Q 20
 ip address 10.10.121.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_Security
 standby 20 ip 10.10.121.1
 standby 20 priority 101
 standby 20 preempt
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.21
 description HIPAA
 encapsulation dot1Q 21
 ip address 10.10.122.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_HIPAA
 standby 21 ip 10.10.122.1
 standby 21 priority 101
 standby 21 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.22
 description WIRELESS-HIPAA-USERS
```

```
 encapsulation dot1Q 22
 ip address 10.10.123.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_HIPAA-WU
 standby 22 ip 10.10.123.1
 standby 22 priority 101
 standby 22 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.23
 description WIRELESS-HIPAA-DEVICES
 encapsulation dot1Q 23
 ip address 10.10.124.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_HIPAA-WD
 standby 23 ip 10.10.124.1
 standby 23 priority 101
 standby 23 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.102
 description ROUTER LINK TO
 encapsulation dot1Q 102
 ip address 10.10.126.29 255.255.255.252
 ip pim sparse-dense-mode
 zone-member security S_R-2-R
 service-policy input BRANCH-LAN-EDGE-IN
!
interface GigabitEthernet0/1.1000
 description MANAGEMENT
 encapsulation dot1Q 1000
 ip address 10.10.127.2 255.255.255.0
 zone-member security S_MGMT
 standby 100 ip 10.10.127.1
 standby 100 priority 101
 standby 100 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/2.101
 description ROUTER LINK TO
 encapsulation dot1Q 101
 ip address 10.10.126.25 255.255.255.252
 ip pim sparse-dense-mode
 zone-member security S_R-2-R
 service-policy input BRANCH-LAN-EDGE-IN
!
interface SM1/0
 ip address 10.10.126.41 255.255.255.252
 zone-member security S_WAAS
 service-module fail-open
 service-module ip address 10.10.126.42 255.255.255.252
 service-module ip default-gateway 10.10.126.41
 hold-queue 60 out
!
```

```
interface SM1/1
 description Internal switch interface connected to Service Module
!
interface Vlan1
 no ip address
!
!
router ospf 5
 router-id 10.10.126.1
 redistribute connected subnets
 passive-interface default
 no passive-interface GigabitEthernet0/1.102
 no passive-interface GigabitEthernet0/2.101
 network 10.10.0.0 0.0.255.255 area 10
 default-information originate
!
no ip forward-protocol nd
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication CiscoACS
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip route 0.0.0.0 0.0.0.0 10.10.255.11
ip tacacs source-interface Loopback0
!
ip access-list extended BULK-DATA-APPS
 remark ---File Transfer---
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
 remark ---E-mail traffic---
 permit tcp any any eq smtp
 permit tcp any any eq pop3
 permit tcp any any eq 143
 remark ---other EDM app protocols---
 permit tcp any any range 3460 3466
 permit tcp any range 3460 3466 any
 remark ---messaging services---
 permit tcp any any eq 2980
 permit tcp any eq 2980 any
 remark ---Microsoft file services---
 permit tcp any any range 137 139
 permit tcp any range 137 139 any
ip access-list extended CSM_ZBF_CMAP_ACL_1
 remark Data Center Mgmt to Devices
 permit object-group CSM_INLINE_svc_rule_81604380993 object-group
CSM_INLINE_src_rule_81604380993 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_10
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381011 object-group DC-POS-Oracle
object-group BRANCH-POS
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381015 object-group DC-POS-SAP object-group
BRANCH-POS
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381019 object-group DC-POS-Tomax
object-group BRANCH-POS
ip access-list extended CSM_ZBF_CMAP_ACL_11
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381021 object-group
CSM_INLINE_src_rule_81604381021 object-group BRANCH-POS
ip access-list extended CSM_ZBF_CMAP_ACL_12
```

```
 remark Data Center VOICE (wired and Wireless)
 permit object-group CSM_INLINE_svc_rule_81604381057 object-group DC-Voice object-group
Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_13
 permit ospf object-group CSM_INLINE_src_rule_81604381150 object-group
CSM_INLINE_dst_rule_81604381150
ip access-list extended CSM_ZBF_CMAP_ACL_14
 remark Store WAAS to Clients and Servers
 permit object-group CSM_INLINE_svc_rule_81604381055 object-group Branches-ALL
object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_15
 permit ospf object-group CSM_INLINE_src_rule_81604381152 object-group
CSM_INLINE_dst_rule_81604381152
ip access-list extended CSM_ZBF_CMAP_ACL_16
 remark Syslog and SNMP Alerts
 permit object-group CSM_INLINE_svc_rule_81604380995 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_81604380995
ip access-list extended CSM_ZBF_CMAP_ACL_17
 remark Store to Data Center Authentications
 permit object-group CSM_INLINE_svc_rule_81604381001 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_81604381001
ip access-list extended CSM_ZBF_CMAP_ACL_18
 remark Store to Data Center for NTP
 permit object-group NTP object-group Branches-ALL object-group NTP-Servers
ip access-list extended CSM_ZBF_CMAP_ACL_19
 remark Store to Data Center for DHCP and DNS
 permit object-group CSM_INLINE_svc_rule_81604381035 object-group Branches-ALL
object-group ActiveDirectory.cisco-irn.com
ip access-list extended CSM_ZBF_CMAP_ACL_2
 remark Data Center subscribe to IPS SDEE events
 permit tcp object-group RSA-enVision object-group Branches-ALL eq 443
ip access-list extended CSM_ZBF_CMAP_ACL_20
 remark Permit ICMP traffic
 permit object-group CSM_INLINE_svc_rule_81604381039 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_81604381039
ip access-list extended CSM_ZBF_CMAP_ACL_21
 remark Store UCS E-series server to Data Center vShphere
 permit object-group CSM_INLINE_svc_rule_81604381005 object-group Branches-ALL
object-group vSphere-1
ip access-list extended CSM_ZBF_CMAP_ACL_22
 remark Store NAC
 permit object-group CSM_INLINE_svc_rule_81604381037 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_81604381037
ip access-list extended CSM_ZBF_CMAP_ACL_23
 remark Store to Data Center Physical Security
 permit ip object-group Branches-ALL object-group CSM_INLINE_dst_rule_81604381049
ip access-list extended CSM_ZBF_CMAP_ACL_24
 remark Store WAAS (WAAS Devices need their own zone)
 permit object-group CSM_INLINE_svc_rule_81604381053 object-group Branches-ALL
object-group DC-WAAS
ip access-list extended CSM_ZBF_CMAP_ACL_25
 remark Store to Data Center wireless controller traffic
 permit object-group CSM_INLINE_svc_rule_81604381045 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_81604381045
ip access-list extended CSM_ZBF_CMAP_ACL_26
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381009 object-group BRANCH-POS object-group
DC-POS-Oracle
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381013 object-group BRANCH-POS object-group
DC-POS-SAP
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381017 object-group BRANCH-POS object-group
DC-POS-Tomax
```

```
ip access-list extended CSM_ZBF_CMAP_ACL_27
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381023 object-group
CSM_INLINE_src_rule_81604381023 object-group BRANCH-POS
ip access-list extended CSM_ZBF_CMAP_ACL_28
 remark Store to Data Center for E-mail
 permit object-group CSM_INLINE_svc_rule_81604381025 object-group BRANCH-POS object-group
MSExchange
ip access-list extended CSM_ZBF_CMAP_ACL_29
 remark Store to Data Center for Windows Updates
 permit object-group CSM_INLINE_svc_rule_81604381027 object-group BRANCH-POS object-group
MS-Update
ip access-list extended CSM_ZBF_CMAP_ACL_3
 remark Permit ICMP traffic
 permit object-group CSM_INLINE_svc_rule_81604381041 object-group
CSM_INLINE_src_rule_81604381041 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_30
 remark Permit POS clients to talk to branch POS server
 permit object-group CSM_INLINE_svc_rule_81604381029 object-group BRANCH-POS object-group
BRANCH-POS
ip access-list extended CSM_ZBF_CMAP_ACL_31
 remark Store to Data Center for Windows Updates
 permit object-group CSM_INLINE_svc_rule_81604381061 object-group Branches-ALL
object-group MS-Update
ip access-list extended CSM_ZBF_CMAP_ACL_32
 remark Store to Data Center for E-mail
 permit object-group CSM_INLINE_svc_rule_81604381063 object-group Branches-ALL
object-group MSExchange
ip access-list extended CSM_ZBF_CMAP_ACL_33
 remark Store DATA (wired and Wireless - Access to DC Other applications)
 permit object-group CSM_INLINE_svc_rule_81604381065 object-group Branches-ALL
object-group DC-Applications
ip access-list extended CSM_ZBF_CMAP_ACL_34
 remark Store GUEST - Drop Traffic to Enterprise
 permit ip object-group Branches-ALL object-group CSM_INLINE_dst_rule_81604381071
ip access-list extended CSM_ZBF_CMAP_ACL_35
 remark Store GUEST (access to internet/DMZ web servers)
 permit ip object-group Branches-ALL any
ip access-list extended CSM_ZBF_CMAP_ACL_36
 remark Store PARTNERS - Drop Traffic to Enterprise
 permit ip object-group Branches-ALL object-group CSM_INLINE_dst_rule_81604381067
ip access-list extended CSM_ZBF_CMAP_ACL_37
 remark Store PARTNERS (wired and wireless - Access to Partner site, Internet VPN)
 permit ip object-group Branches-ALL any
ip access-list extended CSM_ZBF_CMAP_ACL_38
 remark Store VOICE (wired and Wireless - Acess to corporate wide voice)
 permit object-group CSM_INLINE_svc_rule_81604381059 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_81604381059
ip access-list extended CSM_ZBF_CMAP_ACL_4
 remark Data Center vSphere to UCS E-series server
 permit object-group CSM_INLINE_svc_rule_81604381003 object-group vSphere-1 object-group
Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_5
 remark Data Center to Store Physical Security
 permit ip object-group CSM_INLINE_src_rule_81604381047 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_6
 remark Data Center Mgmt to Devices
 permit object-group RDP object-group DC-Admin object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_7
 remark Data Center WAAS to Store
 permit object-group CSM_INLINE_svc_rule_81604381051 object-group
CSM_INLINE_src_rule_81604381051 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_8
 remark Data Center Wireless Control to AP's and Controllers in branchs
```

```
 permit object-group CSM_INLINE_svc_rule_81604381043 object-group
CSM_INLINE_src_rule_81604381043 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_9
 remark Data Center Mgmt to Devices
 permit object-group RDP object-group DC-Admin object-group BRANCH-POS
ip access-list extended MISSION-CRITICAL-SERVERS
 remark ---POS Applications---
 permit ip any 192.168.52.0 0.0.0.255
ip access-list extended NET-MGMT-APPS
 remark - Router user Authentication - Identifies TACACS Control traffic
 permit tcp any any eq tacacs
 permit tcp any eq tacacs any
ip access-list extended TRANSACTIONAL-DATA-APPS
 remark ---Workbrain Application---
 remark --Large Store Clock Server to Central Clock Application
 permit tcp host 10.10.49.94 host 192.168.46.72 eq 8444
 remark --Large branch Clock Server to CUAE
 permit tcp host 10.10.49.94 host 192.168.45.185 eq 8000
 remark ---LiteScape Application---
 permit ip any host 192.168.46.82
 permit ip any 239.192.0.0 0.0.0.255
 permit ip any host 239.255.255.250
 remark ---Remote Desktop---
 permit tcp any any eq 3389
 permit tcp any eq 3389 any
 remark ---Oracle SIM---
 permit tcp any 192.168.46.0 0.0.0.255 eq 7777
 permit tcp any 192.168.46.0 0.0.0.255 eq 6003
 permit tcp any 192.168.46.0 0.0.0.255 range 12401 12500
 permit tcp 192.168.46.0 0.0.0.255 eq 7777 any
 permit tcp 192.168.46.0 0.0.0.255 eq 6003 any
 permit tcp 192.168.46.0 0.0.0.255 range 12401 12500 any
!
logging esm config
logging trap debugging
logging source-interface Loopback0
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
!
!
!
nls resp-timeout 1
cpd cr-id 1
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

```
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps flash insertion removal
snmp-server enable traps energywise
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps ipsla
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server domain-stripping
tacacs-server key 7 <removed>
!
!
control-plane
!
!
!
mgcp fax t38 ecm
!
mgcp profile default
!
!
!
!
!
gatekeeper
 shutdown
!
!
banner exec C
WARNING:
**** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
**** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner incoming C
WARNING:
**** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
**** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
```

```
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.


banner login C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY



!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication CiscoACS
line aux 0
 session-timeout 1  output
 exec-timeout 0 1
 privilege level 0
 login authentication CiscoACS
 no exec
 transport preferred none
 transport output none
line 67
 no activation-character
 no exec
 transport preferred none
 transport input ssh
 transport output none
 stopbits 1
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
ntp source Loopback0
ntp update-calendar
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162
end
```

R-A2-MED-2

```
version 15.1
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname R-A2-MED-2
!
boot-start-marker
boot system flash:c2951-universalk9-mz.SPA.151-3.T.bin
boot-end-marker
!
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 500000
no logging rate-limit
enable secret 5 <removed>
!
aaa new-model
!
!
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default
 action-type start-stop
 group tacacs+
!
aaa accounting commands 15 default
 action-type start-stop
 group tacacs+
!
aaa accounting system default
 action-type start-stop
 group tacacs+
!
!
!
!
!
!
aaa session-id common
!
clock timezone PCTime -8 0
clock summer-time PCTime date Apr 6 2003 2:00 Oct 26 2003 2:00
!
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-104836678
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-104836678
 revocation-check none
!
!
crypto pki certificate chain TP-self-signed-104836678
```

```
 certificate self-signed 02
  <removed>
    quit
no ipv6 cef
no ip source-route
no ip gratuitous-arps
ip cef
!
!
!
ip multicast-routing
!
!
no ip bootp server
ip domain name cisco-irn.com
ip name-server 192.168.42.130
ip port-map user-8443 port tcp 8443
ip ips notify SDEE
ip ips name COMPLIANCE-XXX
!
ip ips signature-category
  category all
   retired true
  category ios_ips default
   retired false
!
ip wccp 61
ip wccp 62
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
multilink bundle-name authenticated
!
parameter-map type inspect global
 WAAS enable
parameter-map type inspect Inspect-1
 audit-trail on

parameter-map type trend-global trend-glob-map
!
!
!
!
password encryption aes
voice-card 0
!
!
!
!
!
!
!
license udi pid CISCO2951/K9 sn <removed>
hw-module sm 1
!
hw-module sm 2
!
!
!
archive
 log config
  logging enable
```

```
  notify syslog contenttype plaintext
  hidekeys
object-group network ActiveDirectory.cisco-irn.com
 host 192.168.42.130
!
object-group service CAPWAP
 description CAPWAP UDP ports 5246 and 5247
 udp eq 5246
 udp eq 5247
!
object-group service CISCO-WAAS
 description Ports for Cisco WAAS
 tcp eq 4050
!
object-group network EMC-NCM
 description EMC Network Configuration Manager
 host 192.168.42.122
!
object-group network RSA-enVision
 description RSA EnVision Syslog collector and SIM
 host 192.168.42.124
!
object-group network CSM_INLINE_dst_rule_81604380995
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object EMC-NCM
 group-object RSA-enVision
!
object-group network TACACS
 description Csico Secure ACS server for TACACS and Radius
 host 192.168.42.131
!
object-group network RSA-AM
 description RSA Authentication Manager for SecureID
 host 192.168.42.137
!
object-group network NAC-1
 description ISE server for NAC
 host 192.168.42.111
!
object-group network CSM_INLINE_dst_rule_81604381001
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object ActiveDirectory.cisco-irn.com
 group-object TACACS
 group-object RSA-AM
 group-object NAC-1
!
object-group network NAC-2
 host 192.168.42.112
!
object-group network CSM_INLINE_dst_rule_81604381037
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object NAC-2
 group-object NAC-1
!
object-group network DC-ALL
 description All of the Data Center
 192.168.0.0 255.255.0.0
!
object-group network Branches-ALL
 description all branch networks
 10.10.0.0 255.255.0.0
!
object-group network CSM_INLINE_dst_rule_81604381039
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
```

```
 group-object DC-ALL
 group-object Branches-ALL
!
object-group network WCSManager
 description Wireless Manager
 host 192.168.43.135
!
object-group network DC-Wifi-Controllers
 description Central Wireless Controllers for branchs
 host 192.168.43.21
 host 192.168.43.22
!
object-group network DC-Wifi-MSE
 description Mobility Service Engines
 host 192.168.43.31
 host 192.168.43.32
!
object-group network CSM_INLINE_dst_rule_81604381045
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
!
object-group network PAME-DC-1
 host 192.168.44.111
!
object-group network MSP-DC-1
 description Data Center VSOM
 host 192.168.44.121
!
object-group network CSM_INLINE_dst_rule_81604381049
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object PAME-DC-1
 group-object MSP-DC-1
!
object-group network CSM_INLINE_dst_rule_81604381059
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
!
object-group network CSM_INLINE_dst_rule_81604381067
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
!
object-group network CSM_INLINE_dst_rule_81604381071
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
!
object-group network CSM_INLINE_dst_rule_81604381150
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 10.10.126.0 255.255.255.0
 10.10.110.0 255.255.255.0
!
object-group network CSM_INLINE_dst_rule_81604381152
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 10.10.126.0 255.255.255.0
 10.10.110.0 255.255.255.0
!
object-group network DC-Admin
 description DC Admin Systems
 host 192.168.41.101
 host 192.168.41.102
```

```
!
object-group network CSManager
 description Cisco Security Manager
 host 192.168.42.133
!
object-group network CSM_INLINE_src_rule_81604380993
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-Admin
 group-object EMC-NCM
 group-object CSManager
!
object-group network DC-POS-Tomax
 description Tomax POS Communication from Store to Data Center
 192.168.52.96 255.255.255.224
!
object-group network DC-POS-SAP
 description SAP POS Communication from Store to Data Center
 192.168.52.144 255.255.255.240
!
object-group network DC-POS-Oracle
 description Oracle POS Communication from Store to Data Center
 192.168.52.128 255.255.255.240
!
object-group network CSM_INLINE_src_rule_81604381021
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-Admin
 group-object DC-POS-Tomax
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
!
object-group network CSM_INLINE_src_rule_81604381023
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-Admin
 group-object DC-POS-Tomax
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
!
object-group network CSM_INLINE_src_rule_81604381041
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
!
object-group network CSM_INLINE_src_rule_81604381043
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
!
object-group network CSM_INLINE_src_rule_81604381047
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object PAME-DC-1
 group-object MSP-DC-1
!
object-group network DC-WAAS
 description WAE Appliances in Data Center
 host 192.168.48.10
 host 192.168.49.10
 host 192.168.47.11
 host 192.168.47.12
!
object-group network CSM_INLINE_src_rule_81604381051
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 group-object DC-Admin
 group-object DC-WAAS
```

```
!
object-group network CSM_INLINE_src_rule_81604381150
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 10.10.126.0 255.255.255.0
 10.10.110.0 255.255.255.0
!
object-group network CSM_INLINE_src_rule_81604381152
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-HA_v1/mandatory)
 10.10.126.0 255.255.255.0
 10.10.110.0 255.255.255.0
!
object-group service CSM_INLINE_svc_rule_81604380993
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
!
object-group service CSM_INLINE_svc_rule_81604380995
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 udp eq syslog
 udp eq snmp
 udp eq snmptrap
!
object-group service CSM_INLINE_svc_rule_81604381001
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq tacacs
 udp eq 1812
 udp eq 1813
 tcp eq 389
 tcp eq 636
!
object-group service vCenter-to-ESX4
 description Communication from vCetner to ESX hosts
 tcp eq 5989
 tcp eq 8000
 tcp eq 902
 tcp eq 903
!
object-group service CSM_INLINE_svc_rule_81604381003
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq 22
 group-object vCenter-to-ESX4
!
object-group service ESX-SLP
 description CIM Service Location Protocol (SLP) for VMware systems
 udp eq 427
 tcp eq 427
!
object-group service CSM_INLINE_svc_rule_81604381005
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 group-object vCenter-to-ESX4
 group-object ESX-SLP
!
object-group service ORACLE-RMI
 description RMI TCP ports 1300 and 1301-1319.
 tcp range 1300 1319
!
```

```
object-group service ORACLE-Weblogic
 description HTTP/RMI and HTTPS/RMI-SSL 7001 & 7002. OracleAQ uses 1521.
 tcp eq 7001
 tcp eq 7002
 tcp eq 1521
!
object-group service ORACLE-WAS
 description RMI/IIOP over 2809  HTTP over 9443 IBM-MQ 1414
 tcp eq 2809
 tcp eq 9443
 tcp eq 1414
!
object-group service ORACLE-OAS
 description OAS uses one port for HTTP and RMI - 12601.
 tcp eq 12601
!
object-group service CSM_INLINE_svc_rule_81604381009
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
 group-object ORACLE-RMI
 group-object ORACLE-Weblogic
 group-object ORACLE-WAS
 group-object ORACLE-OAS
!
object-group service CSM_INLINE_svc_rule_81604381011
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
 group-object ORACLE-RMI
 group-object ORACLE-Weblogic
 group-object ORACLE-WAS
 group-object ORACLE-OAS
!
object-group service HTTPS-8443
 tcp eq 8443
!
object-group service CSM_INLINE_svc_rule_81604381013
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
 group-object HTTPS-8443
!
object-group service CSM_INLINE_svc_rule_81604381015
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq 22
 group-object HTTPS-8443
!
object-group service TOMAX-8990
 description Tomax Application Port
 tcp eq 8990
!
object-group service CSM_INLINE_svc_rule_81604381017
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 group-object TOMAX-8990
!
object-group service CSM_INLINE_svc_rule_81604381019
```

```
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 group-object TOMAX-8990
!
object-group service ICMP-Requests
 description ICMP requests
 icmp information-request
 icmp mask-request
 icmp timestamp-request
!
object-group service CSM_INLINE_svc_rule_81604381021
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
 icmp redirect
 icmp alternate-address
 group-object ICMP-Requests
!
object-group service CSM_INLINE_svc_rule_81604381023
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
 icmp redirect
 icmp alternate-address
 group-object ICMP-Requests
!
object-group service CSM_INLINE_svc_rule_81604381025
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq smtp
 tcp eq pop3
 tcp eq 143
!
object-group service CSM_INLINE_svc_rule_81604381027
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_81604381029
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp
 udp
 tcp eq 443
!
object-group service DNS-Resolving
 description Domain Name Server
 tcp eq domain
 udp eq domain
!
object-group service CSM_INLINE_svc_rule_81604381035
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 udp eq bootps
```

```
 group-object DNS-Resolving
!
object-group service CSM_INLINE_svc_rule_81604381037
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
 group-object HTTPS-8443
!
object-group service CSM_INLINE_svc_rule_81604381039
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
!
object-group service CSM_INLINE_svc_rule_81604381041
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
!
object-group service LWAPP
 description LWAPP UDP ports 12222 and 12223
 udp eq 12222
 udp eq 12223
!
object-group service TFTP
 description Trivial File Transfer
 tcp eq 69
 udp eq tftp
!
object-group service IP-Protocol-97
 description IP protocol 97
 97
!
object-group service CSM_INLINE_svc_rule_81604381043
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq 443
 tcp eq www
 tcp eq 22
 tcp eq telnet
 udp eq isakmp
 group-object CAPWAP
 group-object LWAPP
 group-object TFTP
 group-object IP-Protocol-97
!
object-group service Cisco-Mobility
 description Mobility ports for Wireless
 udp eq 16666
 udp eq 16667
!
object-group service CSM_INLINE_svc_rule_81604381045
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 udp eq isakmp
 group-object CAPWAP
 group-object LWAPP
 group-object Cisco-Mobility
```

```
 group-object IP-Protocol-97
!
object-group service Microsoft-DS-SMB
 description Microsoft-DS Active Directory, Windows shares Microsoft-DS SMB file sharing
 tcp eq 445
!
object-group service CSM_INLINE_svc_rule_81604381051
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp
 tcp eq 139
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_81604381053
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp
 tcp eq 139
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_81604381055
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp
 tcp eq 139
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_81604381057
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 icmp
 tcp-udp eq 5060
 tcp eq 2000
 tcp eq www
 tcp eq 443
 group-object TFTP
!
object-group service CSM_INLINE_svc_rule_81604381059
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp-udp eq 5060
 tcp eq 2000
!
object-group service CSM_INLINE_svc_rule_81604381061
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_81604381063
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq smtp
 tcp eq pop3
 tcp eq 143
!
object-group service Netbios
 description Netbios Servers
```

```
 udp eq netbios-dgm
 udp eq netbios-ns
 tcp eq 139
!
object-group service ORACLE-SIM
 description Oracle Store Inventory Management
 tcp eq 7777
 tcp eq 6003
 tcp range 12401 12500
!
object-group service RDP
 description Windows Remote Desktop
 tcp eq 3389
!
object-group service Workbrain
 tcp eq 8444
!
object-group service CSM_INLINE_svc_rule_81604381065
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-HA_v1/mandatory)
 tcp eq ftp
 tcp eq www
 tcp eq 443
 udp eq 88
 tcp-udp eq 42
 group-object Microsoft-DS-SMB
 group-object Netbios
 group-object ORACLE-SIM
 group-object RDP
 group-object Workbrain
!
object-group network DC-Applications
 description Applications in the Data Center
 192.168.180.0 255.255.254.0
!
object-group network DC-Voice
 description Data Center Voice
 192.168.45.0 255.255.255.0
!
object-group network MS-Update
 description Windows Update Server
 host 192.168.42.150
!
object-group network MSExchange
 description Mail Server
 host 192.168.42.140
!
object-group service NTP
 description NTP Protocols
 tcp eq 123
 udp eq ntp
!
object-group network NTP-Servers
 description NTP Servers
 host 192.168.62.161
 host 162.168.62.162
!
object-group network BRANCH-POS
 10.10.0.0 255.255.0.0
!
object-group network vSphere-1
 description vSphere server for Lab
 host 192.168.41.102
!
```

```
username bart privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
redundancy
!
!
!
!
ip tcp synwait-time 10
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh version 2
ip scp server enable
!
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_7
 match protocol http
 match protocol https
 match protocol microsoft-ds
 match protocol ms-sql
 match protocol ms-sql-m
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol oracle
 match protocol oracle-em-vp
 match protocol oraclenames
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_10
 match access-group name CSM_ZBF_CMAP_ACL_10
 match class-map CSM_ZBF_CMAP_PLMAP_7
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_4
 match protocol http
 match protocol https
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_23
 match access-group name CSM_ZBF_CMAP_ACL_23
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_17
 match protocol http
 match protocol https
 match protocol imap3
 match protocol pop3
 match protocol pop3s
 match protocol smtp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_32
 match access-group name CSM_ZBF_CMAP_ACL_32
 match class-map CSM_ZBF_CMAP_PLMAP_17
class-map type inspect match-all CSM_ZBF_CLASS_MAP_11
 match access-group name CSM_ZBF_CMAP_ACL_11
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_14
 match protocol http
 match protocol https
 match protocol user-8443
class-map type inspect match-all CSM_ZBF_CLASS_MAP_22
 match access-group name CSM_ZBF_CMAP_ACL_22
 match class-map CSM_ZBF_CMAP_PLMAP_14
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_20
 match protocol http
```

```
 match protocol https
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
 match protocol ftp
 match protocol ssh
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_33
 match access-group name CSM_ZBF_CMAP_ACL_33
 match class-map CSM_ZBF_CMAP_PLMAP_20
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_8
 match protocol sip
 match protocol sip-tls
 match protocol skinny
 match protocol tftp
 match protocol http
 match protocol https
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_12
 match access-group name CSM_ZBF_CMAP_ACL_12
 match class-map CSM_ZBF_CMAP_PLMAP_8
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_13
 match protocol https
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_21
 match access-group name CSM_ZBF_CMAP_ACL_21
 match class-map CSM_ZBF_CMAP_PLMAP_13
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_19
 match protocol http
 match protocol https
 match protocol icmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_30
 match access-group name CSM_ZBF_CMAP_ACL_30
 match class-map CSM_ZBF_CMAP_PLMAP_19
class-map type inspect match-all CSM_ZBF_CLASS_MAP_13
 match access-group name CSM_ZBF_CMAP_ACL_13
class-map type inspect match-all CSM_ZBF_CLASS_MAP_20
 match access-group name CSM_ZBF_CMAP_ACL_20
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_18
 match protocol http
 match protocol https
 match protocol udp
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_31
 match access-group name CSM_ZBF_CMAP_ACL_31
 match class-map CSM_ZBF_CMAP_PLMAP_18
class-map match-all BRANCH-BULK-DATA
 match protocol tftp
 match protocol nfs
 match access-group name BULK-DATA-APPS
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_5
 match protocol http
 match protocol https
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_14
 match access-group name CSM_ZBF_CMAP_ACL_14
```

```
 match class-map CSM_ZBF_CMAP_PLMAP_5
class-map type inspect match-all CSM_ZBF_CLASS_MAP_27
 match access-group name CSM_ZBF_CMAP_ACL_27
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_36
 match access-group name CSM_ZBF_CMAP_ACL_36
class-map type inspect match-all CSM_ZBF_CLASS_MAP_15
 match access-group name CSM_ZBF_CMAP_ACL_15
class-map type inspect match-all CSM_ZBF_CLASS_MAP_26
 match access-group name CSM_ZBF_CMAP_ACL_26
 match class-map CSM_ZBF_CMAP_PLMAP_7
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_21
 match protocol tcp
 match protocol udp
 match protocol http
 match protocol https
class-map type inspect match-all CSM_ZBF_CLASS_MAP_37
 match access-group name CSM_ZBF_CMAP_ACL_37
 match class-map CSM_ZBF_CMAP_PLMAP_21
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_9
 match protocol syslog
 match protocol syslog-conn
 match protocol snmp
 match protocol snmptrap
class-map type inspect match-all CSM_ZBF_CLASS_MAP_16
 match access-group name CSM_ZBF_CMAP_ACL_16
 match class-map CSM_ZBF_CMAP_PLMAP_9
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_16
 match protocol http
 match protocol https
 match protocol isakmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_25
 match access-group name CSM_ZBF_CMAP_ACL_25
 match class-map CSM_ZBF_CMAP_PLMAP_16
class-map type inspect match-all CSM_ZBF_CLASS_MAP_34
 match access-group name CSM_ZBF_CMAP_ACL_34
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_10
 match protocol ldaps
 match protocol ldap
 match protocol ldap-admin
 match protocol radius
 match protocol tacacs
 match protocol tacacs-ds
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_17
 match access-group name CSM_ZBF_CMAP_ACL_17
 match class-map CSM_ZBF_CMAP_PLMAP_10
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_15
 match protocol http
 match protocol https
 match protocol netbios-ns
 match protocol netbios-dgm
 match protocol netbios-ssn
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_24
 match access-group name CSM_ZBF_CMAP_ACL_24
 match class-map CSM_ZBF_CMAP_PLMAP_15
class-map type inspect match-all CSM_ZBF_CLASS_MAP_35
 match access-group name CSM_ZBF_CMAP_ACL_35
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_11
```

```
 match protocol ntp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_18
 match access-group name CSM_ZBF_CMAP_ACL_18
 match class-map CSM_ZBF_CMAP_PLMAP_11
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_12
 match protocol bootpc
 match protocol bootps
 match protocol udp
 match protocol tcp
 match protocol dns
 match protocol dhcp-failover
class-map type inspect match-all CSM_ZBF_CLASS_MAP_19
 match access-group name CSM_ZBF_CMAP_ACL_19
 match class-map CSM_ZBF_CMAP_PLMAP_12
class-map type inspect match-all CSM_ZBF_CLASS_MAP_29
 match access-group name CSM_ZBF_CMAP_ACL_29
 match class-map CSM_ZBF_CMAP_PLMAP_18
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_22
 match protocol sip
 match protocol sip-tls
 match protocol skinny
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_38
 match access-group name CSM_ZBF_CMAP_ACL_38
 match class-map CSM_ZBF_CMAP_PLMAP_22
class-map type inspect match-all CSM_ZBF_CLASS_MAP_28
 match access-group name CSM_ZBF_CMAP_ACL_28
 match class-map CSM_ZBF_CMAP_PLMAP_17
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_1
 match protocol https
 match protocol ssh
class-map type inspect match-all CSM_ZBF_CLASS_MAP_1
 match access-group name CSM_ZBF_CMAP_ACL_1
 match class-map CSM_ZBF_CMAP_PLMAP_1
class-map type inspect match-all CSM_ZBF_CLASS_MAP_3
 match access-group name CSM_ZBF_CMAP_ACL_3
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_2
 match protocol https
 match protocol http
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_2
 match access-group name CSM_ZBF_CMAP_ACL_2
 match class-map CSM_ZBF_CMAP_PLMAP_2
class-map type inspect match-all CSM_ZBF_CLASS_MAP_5
 match access-group name CSM_ZBF_CMAP_ACL_5
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_3
 match protocol http
 match protocol https
 match protocol ssh
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_4
 match access-group name CSM_ZBF_CMAP_ACL_4
 match class-map CSM_ZBF_CMAP_PLMAP_3
class-map type inspect match-all CSM_ZBF_CLASS_MAP_7
 match access-group name CSM_ZBF_CMAP_ACL_7
 match class-map CSM_ZBF_CMAP_PLMAP_5
class-map type inspect match-all CSM_ZBF_CLASS_MAP_6
 match access-group name CSM_ZBF_CMAP_ACL_6
```

```
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_9
 match access-group name CSM_ZBF_CMAP_ACL_9
 match protocol tcp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_6
 match protocol http
 match protocol https
 match protocol ssh
 match protocol telnet
 match protocol tftp
 match protocol isakmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_8
 match access-group name CSM_ZBF_CMAP_ACL_8
 match class-map CSM_ZBF_CMAP_PLMAP_6
class-map match-all BULK-DATA
 match ip dscp af11  af12
class-map match-all INTERACTIVE-VIDEO
 match ip dscp af41  af42
class-map match-any BRANCH-TRANSACTIONAL-DATA
 match protocol citrix
 match protocol ldap
 match protocol telnet
 match protocol sqlnet
 match protocol http url "*SalesReport*"
 match access-group name TRANSACTIONAL-DATA-APPS
class-map match-all BRANCH-MISSION-CRITICAL
 match access-group name MISSION-CRITICAL-SERVERS
class-map match-all VOICE
 match ip dscp ef
class-map match-all MISSION-CRITICAL-DATA
 match ip dscp 25
class-map match-any BRANCH-NET-MGMT
 match protocol snmp
 match protocol syslog
 match protocol dns
 match protocol icmp
 match protocol ssh
 match access-group name NET-MGMT-APPS
class-map match-all ROUTING
 match ip dscp cs6
class-map match-all SCAVENGER
 match ip dscp cs1
class-map match-all NET-MGMT
 match ip dscp cs2
class-map match-any BRANCH-SCAVENGER
 match protocol gnutella
 match protocol fasttrack
 match protocol kazaa2
class-map match-any CALL-SIGNALING
 match ip dscp cs3
class-map match-all TRANSACTIONAL-DATA
 match ip dscp af21  af22
!
!
policy-map BRANCH-LAN-EDGE-OUT
 class class-default
policy-map BRANCH-WAN-EDGE
 class VOICE
  priority percent 18
 class INTERACTIVE-VIDEO
  priority percent 15
 class CALL-SIGNALING
```

```
  bandwidth percent 5
 class ROUTING
  bandwidth percent 3
 class NET-MGMT
  bandwidth percent 2
 class MISSION-CRITICAL-DATA
  bandwidth percent 15
  random-detect
 class TRANSACTIONAL-DATA
  bandwidth percent 12
  random-detect dscp-based
 class BULK-DATA
  bandwidth percent 4
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 1
 class class-default
  bandwidth percent 25
  random-detect
policy-map type inspect CSM_ZBF_POLICY_MAP_18
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_19
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_25
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_16
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_23
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_25
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
```

```
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_32
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_36
  drop log
 class type inspect CSM_ZBF_CLASS_MAP_37
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_17
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_24
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_24
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_34
  drop log
 class type inspect CSM_ZBF_CLASS_MAP_35
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_14
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_27
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_15
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_21
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
```

```
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_26
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_38
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_12
 class type inspect CSM_ZBF_CLASS_MAP_15
  pass
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_21
 class type inspect CSM_ZBF_CLASS_MAP_27
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_28
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_29
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_13
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_20
 class type inspect CSM_ZBF_CLASS_MAP_26
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_27
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_28
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_29
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
```

```
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_10
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_23
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_31
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_32
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_33
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_11
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_22
 class type inspect CSM_ZBF_CLASS_MAP_30
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_9
 class type inspect CSM_ZBF_CLASS_MAP_13
  pass
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_8
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_12
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_7
 class type inspect CSM_ZBF_CLASS_MAP_9
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_10
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_11
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_6
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
```

```
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_5
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_8
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_4
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_7
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_3
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_5
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_2
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_4
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_1
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_2
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop
policy-map BRANCH-LAN-EDGE-IN
 class BRANCH-MISSION-CRITICAL
  set ip dscp 25
 class BRANCH-TRANSACTIONAL-DATA
  set ip dscp af21
 class BRANCH-NET-MGMT
  set ip dscp cs2
 class BRANCH-BULK-DATA
  set ip dscp af11
 class BRANCH-SCAVENGER
  set ip dscp cs1
!
zone security S_WAN
 description Store WAN Link
```

```
zone security S_R-2-R
 description Bridge link between routers
zone security LOOPBACK
 description Loopback interface
zone security S_MGMT
 description VLAN1000 Management
zone security S_Security
 description VLAN20 Physical Security Systems
zone security S_WAAS
 description VLAN19 WAAS optimization
zone security S_WLC-AP
 description VLAN18 Wireless Systems
zone security S_Data
 description VLAN12 Store Data
zone security S_Data-W
 description VLAN14 Store Wireless Data
zone security S_Guest
 description VLAN17 Guest/Public Wireless
zone security S_Voice
 description VLAN13 Store Voice
zone security S_Partners
 description VLAN16 Partner network
zone security S_POS
 description VLAN 11 POS Data
zone security S_POS-W
 description VLAN15 Store Wireless POS
zone security S_HIPAA
 description VLAN21 HIPAA
zone security S_HIPAA-WU
 description VLAN15 Wireless HIPAA Users
zone security S_HIPAA-WD
 description VLAN15 Wireless HIPAA Devices
zone-pair security CSM_S_WAN-LOOPBACK_1 source S_WAN destination LOOPBACK
 service-policy type inspect CSM_ZBF_POLICY_MAP_1
zone-pair security CSM_S_WAN-S_MGMT_1 source S_WAN destination S_MGMT
 service-policy type inspect CSM_ZBF_POLICY_MAP_2
zone-pair security CSM_S_WAN-S_Security_1 source S_WAN destination S_Security
 service-policy type inspect CSM_ZBF_POLICY_MAP_3
zone-pair security CSM_S_WAN-S_WAAS_1 source S_WAN destination S_WAAS
 service-policy type inspect CSM_ZBF_POLICY_MAP_4
zone-pair security CSM_S_WAN-S_WLC-AP_1 source S_WAN destination S_WLC-AP
 service-policy type inspect CSM_ZBF_POLICY_MAP_5
zone-pair security CSM_S_WAN-S_Data_1 source S_WAN destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Data-W_1 source S_WAN destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Guest_1 source S_WAN destination S_Guest
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Partners_1 source S_WAN destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_POS_1 source S_WAN destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_POS-W_1 source S_WAN destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_HIPAA_1 source S_WAN destination S_HIPAA
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_HIPAA-WU_1 source S_WAN destination S_HIPAA-WU
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_Voice_1 source S_WAN destination S_Voice
 service-policy type inspect CSM_ZBF_POLICY_MAP_8
zone-pair security CSM_S_R-2-R-LOOPBACK_1 source S_R-2-R destination LOOPBACK
 service-policy type inspect CSM_ZBF_POLICY_MAP_1
zone-pair security CSM_S_R-2-R-S_MGMT_1 source S_R-2-R destination S_MGMT
 service-policy type inspect CSM_ZBF_POLICY_MAP_2
```

```
zone-pair security CSM_S_R-2-R-S_Security_1 source S_R-2-R destination S_Security
 service-policy type inspect CSM_ZBF_POLICY_MAP_3
zone-pair security CSM_S_R-2-R-S_WAAS_1 source S_R-2-R destination S_WAAS
 service-policy type inspect CSM_ZBF_POLICY_MAP_4
zone-pair security CSM_S_R-2-R-S_WLC-AP_1 source S_R-2-R destination S_WLC-AP
 service-policy type inspect CSM_ZBF_POLICY_MAP_5
zone-pair security CSM_S_R-2-R-self_1 source S_R-2-R destination self
 service-policy type inspect CSM_ZBF_POLICY_MAP_9
zone-pair security CSM_S_R-2-R-S_Data_1 source S_R-2-R destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_R-2-R-S_Data-W_1 source S_R-2-R destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_R-2-R-S_Guest_1 source S_R-2-R destination S_Guest
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_R-2-R-S_Partners_1 source S_R-2-R destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_R-2-R-S_POS_1 source S_R-2-R destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_R-2-R-S_POS-W_1 source S_R-2-R destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_R-2-R-S_HIPAA_1 source S_R-2-R destination S_HIPAA
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_R-2-R-S_HIPAA-WU _1 source S_R-2-R destination S_HIPAA-WU
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_R-2-R-S_Voice_1 source S_R-2-R destination S_Voice
 service-policy type inspect CSM_ZBF_POLICY_MAP_11
zone-pair security CSM_self-S_R-2-R_1 source self destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_12
zone-pair security CSM_LOOPBACK-S_WAN_1 source LOOPBACK destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_13
zone-pair security CSM_LOOPBACK-S_R-2-R_1 source LOOPBACK destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_13
zone-pair security CSM_LOOPBACK-S_POS_1 source LOOPBACK destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_LOOPBACK-S_POS-W_1 source LOOPBACK destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_MGMT-S_WAN_1 source S_MGMT destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_15
zone-pair security CSM_S_MGMT-S_R-2-R_1 source S_MGMT destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_15
zone-pair security CSM_S_MGMT-S_POS_1 source S_MGMT destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_MGMT-S_POS-W_1 source S_MGMT destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Security-S_WAN_1 source S_Security destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_16
zone-pair security CSM_S_Security-S_R-2-R_1 source S_Security destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_16
zone-pair security CSM_S_Security-S_POS_1 source S_Security destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Security-S_POS-W_1 source S_Security destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_WAN_1 source S_WAAS destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_17
zone-pair security CSM_S_WAAS-S_R-2-R_1 source S_WAAS destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_17
zone-pair security CSM_S_WAAS-S_POS_1 source S_WAAS destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_POS-W_1 source S_WAAS destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_Data_1 source S_WAAS destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
zone-pair security CSM_S_WAAS-S_Data-W_1 source S_WAAS destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
```

```
zone-pair security CSM_S_WAAS-S_Partners_1 source S_WAAS destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
zone-pair security CSM_S_WLC-AP-S_WAN_1 source S_WLC-AP destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_19
zone-pair security CSM_S_WLC-AP-S_R-2-R_1 source S_WLC-AP destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_19
zone-pair security CSM_S_WLC-AP-S_POS_1 source S_WLC-AP destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WLC-AP-S_POS-W_1 source S_WLC-AP destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_POS-S_WAN_1 source S_POS destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_20
zone-pair security CSM_S_POS-S_R-2-R_1 source S_POS destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_20
zone-pair security CSM_S_POS-W-S_WAN_1 source S_POS-W destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_21
zone-pair security CSM_S_POS-W-S_R-2-R_1 source S_POS-W destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_21
zone-pair security CSM_S_POS-W-S_POS_1 source S_POS-W destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_22
zone-pair security CSM_S_Data-S_POS_1 source S_Data destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Data-S_POS-W_1 source S_Data destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Data-S_WAN_1 source S_Data destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_23
zone-pair security CSM_S_Data-S_R-2-R_1 source S_Data destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_23
zone-pair security CSM_S_Data-W-S_POS_1 source S_Data-W destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Data-W-S_POS-W_1 source S_Data-W destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Data-W-S_WAN_1 source S_Data-W destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_23
zone-pair security CSM_S_Data-W-S_R-2-R_1 source S_Data-W destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_23
zone-pair security CSM_S_Guest-S_POS_1 source S_Guest destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Guest-S_POS-W_1 source S_Guest destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Guest-S_WAN_1 source S_Guest destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_24
zone-pair security CSM_S_Guest-S_R-2-R_1 source S_Guest destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_24
zone-pair security CSM_S_Partners-S_POS_1 source S_Partners destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Partners-S_POS-W_1 source S_Partners destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Partners-S_WAN_1 source S_Partners destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_25
zone-pair security CSM_S_Partners-S_R-2-R_1 source S_Partners destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_25
zone-pair security CSM_S_Voice-S_POS_1 source S_Voice destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Voice-S_POS-W_1 source S_Voice destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_Voice-S_WAN_1 source S_Voice destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_26
zone-pair security CSM_S_Voice-S_R-2-R_1 source S_Voice destination S_R-2-R
 service-policy type inspect CSM_ZBF_POLICY_MAP_27
!
interface Loopback0
 ip address 10.10.126.2 255.255.255.255
 ip pim sparse-dense-mode
```

```
 zone-member security LOOPBACK
!
interface GigabitEthernet0/0
 ip address 10.10.254.112 255.255.255.0
 ip ips COMPLIANCE-XXX in
 zone-member security S_WAN
 duplex auto
 speed auto
 service-policy output BRANCH-WAN-EDGE
!
interface GigabitEthernet0/1
 description ROUTER LINK TO SWITCH
 no ip address
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/1.11
 description POS
 encapsulation dot1Q 11
 ip address 10.10.112.3 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_POS
 standby 11 ip 10.10.112.1
 standby 11 priority 99
 standby 11 preempt
 ip igmp query-interval 125
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.12
 description DATA
 encapsulation dot1Q 12
 ip address 10.10.113.3 255.255.255.0
 ip helper-address 192.168.42.130
 ip wccp 61 redirect in
 ip pim sparse-dense-mode
 zone-member security S_Data
 standby 12 ip 10.10.113.1
 standby 12 priority 99
 standby 12 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.13
 description VOICE
 encapsulation dot1Q 13
 ip address 10.10.114.3 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_Voice
 standby 13 ip 10.10.114.1
 standby 13 priority 99
 standby 13 preempt
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.14
 description WIRELESS
 encapsulation dot1Q 14
 ip address 10.10.115.3 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Data-W
 standby 14 ip 10.10.115.1
```

```
 standby 14 priority 99
 standby 14 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.15
 description WIRELESS-POS
 encapsulation dot1Q 15
 ip address 10.10.116.3 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_POS-W
 standby 15 ip 10.10.116.1
 standby 15 priority 99
 standby 15 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.16
 description PARTNER
 encapsulation dot1Q 16
 ip address 10.10.117.3 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Partners
 standby 16 ip 10.10.117.1
 standby 16 priority 99
 standby 16 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.17
 description WIRELESS-GUEST
 encapsulation dot1Q 17
 ip address 10.10.118.3 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Guest
 standby 17 ip 10.10.118.1
 standby 17 priority 99
 standby 17 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.18
 description WIRELESS-CONTROL
 encapsulation dot1Q 18
 ip address 10.10.119.3 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_WLC-AP
 standby 18 ip 10.10.119.1
 standby 18 priority 99
 standby 18 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.19
 description WAAS
 encapsulation dot1Q 19
 ip address 10.10.120.3 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_WAAS
 standby 19 ip 10.10.120.1
 standby 19 priority 99
 standby 19 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
```

```
!
interface GigabitEthernet0/1.20
 description SECURITY-SYSTEMS
 encapsulation dot1Q 20
 ip address 10.10.121.3 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_Security
 standby 20 ip 10.10.121.1
 standby 20 priority 99
 standby 20 preempt
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.21
 description HIPAA
 encapsulation dot1Q 21
 ip address 10.10.122.3 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_HIPAA
 standby 21 ip 10.10.122.1
 standby 21 priority 101
 standby 21 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.22
 description WIRELESS-HIPAA-USERS
 encapsulation dot1Q 22
 ip address 10.10.123.3 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_HIPAA-WU
 standby 22 ip 10.10.123.1
 standby 22 priority 101
 standby 22 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.23
 description WIRELESS-HIPAA-DEVICES
 encapsulation dot1Q 23
 ip address 10.10.124.3 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_HIPAA-WD
 standby 23 ip 10.10.124.1
 standby 23 priority 101
 standby 23 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.101
 description ROUTER LINK TO
 encapsulation dot1Q 101
 ip address 10.10.126.26 255.255.255.252
 ip pim sparse-dense-mode
 zone-member security S_R-2-R
 service-policy input BRANCH-LAN-EDGE-IN
!
interface GigabitEthernet0/1.1000
 description MANAGEMENT
 encapsulation dot1Q 1000
 ip address 10.10.127.3 255.255.255.0
```

```
 zone-member security S_MGMT
 standby 100 ip 10.10.127.1
 standby 100 priority 99
 standby 100 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/2.102
 description ROUTER LINK TO
 encapsulation dot1Q 102
 ip address 10.10.126.30 255.255.255.252
 ip pim sparse-dense-mode
 zone-member security S_R-2-R
 service-policy input BRANCH-LAN-EDGE-IN
!
interface SM1/0
 description Video Survillance VMSS Module
 ip address 10.10.126.45 255.255.255.252
 zone-member security S_Security
 service-module ip address 10.10.126.46 255.255.255.252
 !Application: FNDN Running on SM
 service-module ip default-gateway 10.10.126.45
 hold-queue 60 out
!
interface SM1/1
 description Internal switch interface connected to Service Module
!
interface SM2/0
 ip address 10.10.126.50 255.255.255.252
 zone-member security S_MGMT
 service-module ip address 10.10.126.49 255.255.255.252
 !Application: SRE-V Running on SMV
 service-module ip default-gateway 10.10.126.50
 service-module mgf ip address 10.10.125.49 255.255.255.0
 hold-queue 60 out
!
interface SM2/1
 description Internal switch interface connected to Service Module
!
interface Vlan1
 description ESXi Host and Virtual Machines$ES_LAN$
 ip address 10.10.125.50 255.255.255.0
 zone-member security S_POS
!
!
router ospf 5
 router-id 10.10.126.2
 redistribute connected subnets
 passive-interface default
 no passive-interface GigabitEthernet0/1.101
 no passive-interface GigabitEthernet0/2.102
 network 10.10.0.0 0.0.255.255 area 10
 default-information originate
!
no ip forward-protocol nd
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication CiscoACS
```

```
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip route 0.0.0.0 0.0.0.0 10.10.254.11
ip tacacs source-interface Loopback0
!
ip access-list extended BULK-DATA-APPS
 remark ---File Transfer---
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
 remark ---E-mail traffic---
 permit tcp any any eq smtp
 permit tcp any any eq pop3
 permit tcp any any eq 143
 remark ---other EDM app protocols---
 permit tcp any any range 3460 3466
 permit tcp any range 3460 3466 any
 remark ---messaging services---
 permit tcp any any eq 2980
 permit tcp any eq 2980 any
 remark ---Microsoft file services---
 permit tcp any any range 137 139
 permit tcp any range 137 139 any
ip access-list extended CSM_ZBF_CMAP_ACL_1
 remark Data Center Mgmt to Devices
 permit object-group CSM_INLINE_svc_rule_81604380993 object-group
CSM_INLINE_src_rule_81604380993 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_10
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381011 object-group DC-POS-Oracle
object-group BRANCH-POS
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381015 object-group DC-POS-SAP object-group
BRANCH-POS
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381019 object-group DC-POS-Tomax
object-group BRANCH-POS
ip access-list extended CSM_ZBF_CMAP_ACL_11
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381021 object-group
CSM_INLINE_src_rule_81604381021 object-group BRANCH-POS
ip access-list extended CSM_ZBF_CMAP_ACL_12
 remark Data Center VOICE (wired and Wireless)
 permit object-group CSM_INLINE_svc_rule_81604381057 object-group DC-Voice object-group
Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_13
 permit ospf object-group CSM_INLINE_src_rule_81604381150 object-group
CSM_INLINE_dst_rule_81604381150
ip access-list extended CSM_ZBF_CMAP_ACL_14
 remark Store WAAS to Clients and Servers
 permit object-group CSM_INLINE_svc_rule_81604381055 object-group Branches-ALL
object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_15
 permit ospf object-group CSM_INLINE_src_rule_81604381152 object-group
CSM_INLINE_dst_rule_81604381152
ip access-list extended CSM_ZBF_CMAP_ACL_16
 remark Syslog and SNMP Alerts
 permit object-group CSM_INLINE_svc_rule_81604380995 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_81604380995
ip access-list extended CSM_ZBF_CMAP_ACL_17
 remark Store to Data Center Authentications
 permit object-group CSM_INLINE_svc_rule_81604381001 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_81604381001
```

```
ip access-list extended CSM_ZBF_CMAP_ACL_18
 remark Store to Data Center for NTP
 permit object-group NTP object-group Branches-ALL object-group NTP-Servers
ip access-list extended CSM_ZBF_CMAP_ACL_19
 remark Store to Data Center for DHCP and DNS
 permit object-group CSM_INLINE_svc_rule_81604381035 object-group Branches-ALL
object-group ActiveDirectory.cisco-irn.com
ip access-list extended CSM_ZBF_CMAP_ACL_2
 remark Data Center subscribe to IPS SDEE events
 permit tcp object-group RSA-enVision object-group Branches-ALL eq 443
ip access-list extended CSM_ZBF_CMAP_ACL_20
 remark Permit ICMP traffic
 permit object-group CSM_INLINE_svc_rule_81604381039 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_81604381039
ip access-list extended CSM_ZBF_CMAP_ACL_21
 remark Store UCS E-series server to Data Center vShphere
 permit object-group CSM_INLINE_svc_rule_81604381005 object-group Branches-ALL
object-group vSphere-1
ip access-list extended CSM_ZBF_CMAP_ACL_22
 remark Store NAC
 permit object-group CSM_INLINE_svc_rule_81604381037 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_81604381037
ip access-list extended CSM_ZBF_CMAP_ACL_23
 remark Store to Data Center Physical Security
 permit ip object-group Branches-ALL object-group CSM_INLINE_dst_rule_81604381049
ip access-list extended CSM_ZBF_CMAP_ACL_24
 remark Store WAAS (WAAS Devices need their own zone)
 permit object-group CSM_INLINE_svc_rule_81604381053 object-group Branches-ALL
object-group DC-WAAS
ip access-list extended CSM_ZBF_CMAP_ACL_25
 remark Store to Data Center wireless controller traffic
 permit object-group CSM_INLINE_svc_rule_81604381045 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_81604381045
ip access-list extended CSM_ZBF_CMAP_ACL_26
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381009 object-group BRANCH-POS object-group
DC-POS-Oracle
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381013 object-group BRANCH-POS object-group
DC-POS-SAP
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381017 object-group BRANCH-POS object-group
DC-POS-Tomax
ip access-list extended CSM_ZBF_CMAP_ACL_27
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_81604381023 object-group
CSM_INLINE_src_rule_81604381023 object-group BRANCH-POS
ip access-list extended CSM_ZBF_CMAP_ACL_28
 remark Store to Data Center for E-mail
 permit object-group CSM_INLINE_svc_rule_81604381025 object-group BRANCH-POS object-group
MSExchange
ip access-list extended CSM_ZBF_CMAP_ACL_29
 remark Store to Data Center for Windows Updates
 permit object-group CSM_INLINE_svc_rule_81604381027 object-group BRANCH-POS object-group
MS-Update
ip access-list extended CSM_ZBF_CMAP_ACL_3
 remark Permit ICMP traffic
 permit object-group CSM_INLINE_svc_rule_81604381041 object-group
CSM_INLINE_src_rule_81604381041 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_30
 remark Permit POS clients to talk to branch POS server
 permit object-group CSM_INLINE_svc_rule_81604381029 object-group BRANCH-POS object-group
BRANCH-POS
ip access-list extended CSM_ZBF_CMAP_ACL_31
```

```
 remark Store to Data Center for Windows Updates
 permit object-group CSM_INLINE_svc_rule_81604381061 object-group Branches-ALL
object-group MS-Update
ip access-list extended CSM_ZBF_CMAP_ACL_32
 remark Store to Data Center for E-mail
 permit object-group CSM_INLINE_svc_rule_81604381063 object-group Branches-ALL
object-group MSExchange
ip access-list extended CSM_ZBF_CMAP_ACL_33
 remark Store DATA (wired and Wireless - Access to DC Other applications)
 permit object-group CSM_INLINE_svc_rule_81604381065 object-group Branches-ALL
object-group DC-Applications
ip access-list extended CSM_ZBF_CMAP_ACL_34
 remark Store GUEST - Drop Traffic to Enterprise
 permit ip object-group Branches-ALL object-group CSM_INLINE_dst_rule_81604381071
ip access-list extended CSM_ZBF_CMAP_ACL_35
 remark Store GUEST (access to internet/DMZ web servers)
 permit ip object-group Branches-ALL any
ip access-list extended CSM_ZBF_CMAP_ACL_36
 remark Store PARTNERS - Drop Traffic to Enterprise
 permit ip object-group Branches-ALL object-group CSM_INLINE_dst_rule_81604381067
ip access-list extended CSM_ZBF_CMAP_ACL_37
 remark Store PARTNERS (wired and wireless - Access to Partner site, Internet VPN)
 permit ip object-group Branches-ALL any
ip access-list extended CSM_ZBF_CMAP_ACL_38
 remark Store VOICE (wired and Wireless - Acess to corporate wide voice)
 permit object-group CSM_INLINE_svc_rule_81604381059 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_81604381059
ip access-list extended CSM_ZBF_CMAP_ACL_4
 remark Data Center vSphere to UCS E-series server
 permit object-group CSM_INLINE_svc_rule_81604381003 object-group vSphere-1 object-group
Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_5
 remark Data Center to Store Physical Security
 permit ip object-group CSM_INLINE_src_rule_81604381047 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_6
 remark Data Center Mgmt to Devices
 permit object-group RDP object-group DC-Admin object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_7
 remark Data Center WAAS to Store
 permit object-group CSM_INLINE_svc_rule_81604381051 object-group
CSM_INLINE_src_rule_81604381051 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_8
 remark Data Center Wireless Control to AP's and Controllers in branchs
 permit object-group CSM_INLINE_svc_rule_81604381043 object-group
CSM_INLINE_src_rule_81604381043 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_9
 remark Data Center Mgmt to Devices
 permit object-group RDP object-group DC-Admin object-group BRANCH-POS
ip access-list extended MISSION-CRITICAL-SERVERS
 remark ---POS Applications---
 permit ip any 192.168.52.0 0.0.0.255
ip access-list extended NET-MGMT-APPS
 remark - Router user Authentication - Identifies TACACS Control traffic
 permit tcp any any eq tacacs
 permit tcp any eq tacacs any
ip access-list extended TRANSACTIONAL-DATA-APPS
 remark ---Workbrain Application---
 remark --Large Store Clock Server to Central Clock Application
 permit tcp host 10.10.49.94 host 192.168.46.72 eq 8444
 remark --Large branch Clock Server to CUAE
 permit tcp host 10.10.49.94 host 192.168.45.185 eq 8000
 remark ---LiteScape Application---
 permit ip any host 192.168.46.82
 permit ip any 239.192.0.0 0.0.0.255
```

```
 permit ip any host 239.255.255.250
 remark ---Remote Desktop---
 permit tcp any any eq 3389
 permit tcp any eq 3389 any
 remark ---Oracle SIM---
 permit tcp any 192.168.46.0 0.0.0.255 eq 7777
 permit tcp any 192.168.46.0 0.0.0.255 eq 6003
 permit tcp any 192.168.46.0 0.0.0.255 range 12401 12500
 permit tcp 192.168.46.0 0.0.0.255 eq 7777 any
 permit tcp 192.168.46.0 0.0.0.255 eq 6003 any
 permit tcp 192.168.46.0 0.0.0.255 range 12401 12500 any
!
logging esm config
logging trap debugging
logging source-interface Loopback0
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
!
!
!
nls resp-timeout 1
cpd cr-id 1
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps flash insertion removal
snmp-server enable traps energywise
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps ipsla
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server domain-stripping
tacacs-server key 7 <removed>
!
```

```
!
control-plane
!
!
!
!
mgcp profile default
!
!
!
!
!
gatekeeper
 shutdown
!
!
banner exec
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner incoming
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner login
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!

!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication CiscoACS
line aux 0
 session-timeout 1  output
 exec-timeout 0 1
 privilege level 0
 login authentication CiscoACS
 no exec
 transport preferred none
 transport output none
line 67
```

```
 no activation-character
 no exec
 transport preferred none
 transport input ssh
 transport output none
 stopbits 1
line 131
 no activation-character
 no exec
 transport preferred none
 transport input ssh
 transport output none
 stopbits 1
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
!
scheduler allocate 20000 1000
scheduler interval 500
ntp source Loopback0
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162
end
```

S-A2-MED-1

```
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname S-A2-MED-1/2
!
boot-start-marker
boot-end-marker
!
logging buffered 50000
enable secret 5 <removed>
!

username bart privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
```

```
username csmadmin privilege 15 secret 5 <removed>
!
!
aaa new-model
!
!
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
switch 1 provision ws-c3750x-48p
switch 2 provision ws-c3750x-48p
system mtu routing 1500
authentication mac-move permit
ip subnet-zero
no ip source-route
no ip gratuitous-arps
!
!
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
password encryption aes
!
crypto pki trustpoint TP-self-signed-4271428864
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-4271428864
 revocation-check none
 rsakeypair TP-self-signed-4271428864
!
!
crypto pki certificate chain TP-self-signed-4271428864
 certificate self-signed 01
  <removed>  quit
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
spanning-tree mode pvst
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 10
ip ssh time-out 30
ip ssh authentication-retries 2
```

```
ip ssh version 2
ip scp server enable
!
!
interface FastEthernet0
 no ip address
 shutdown
!
interface GigabitEthernet1/0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/3
 description Cisco9971 IP phone
 switchport access vlan 11
 switchport trunk encapsulation dot1q
 switchport voice vlan 13
 spanning-tree portfast
!
interface GigabitEthernet1/0/4
 description Cisco7975 IP phone
 switchport access vlan 11
 switchport trunk encapsulation dot1q
 switchport voice vlan 13
 spanning-tree portfast
!
interface GigabitEthernet1/0/5
 switchport access vlan 20
!
interface GigabitEthernet1/0/6
 description CPAM Gateway
 switchport access vlan 20
!
interface GigabitEthernet1/0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/8
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/9
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/10
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/11
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/12
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/13
 switchport access vlan 17
 shutdown
```

```
!
interface GigabitEthernet1/0/14
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/15
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/16
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/17
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/18
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/19
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/20
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/21
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/22
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/23
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/24
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/25
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/26
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/27
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/28
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/29
 switchport access vlan 17
 shutdown
```

```
!
interface GigabitEthernet1/0/30
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/31
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/32
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/33
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/34
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/35
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/36
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/37
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/38
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/39
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/40
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/41
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/42
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/43
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/44
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/45
 switchport access vlan 17
 shutdown
```

```
!
interface GigabitEthernet1/0/46
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/47
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/48
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/1/1
 shutdown
!
interface GigabitEthernet1/1/2
 shutdown
!
interface GigabitEthernet1/1/3
 shutdown
!
interface GigabitEthernet1/1/4
 shutdown
!
interface TenGigabitEthernet1/1/1
 shutdown
!
interface TenGigabitEthernet1/1/2
 shutdown
!
interface GigabitEthernet2/0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet2/0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet2/0/3
!
interface GigabitEthernet2/0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet2/0/5
 description AIR-CAP3502E
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 18
 switchport trunk allowed vlan 14-18
 switchport mode trunk
!
interface GigabitEthernet2/0/6
 description AIR-LAP1262N
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 18
 switchport trunk allowed vlan 14-18
 switchport mode trunk
!
interface GigabitEthernet2/0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet2/0/8
```

```
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/9
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/10
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/11
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/12
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/13
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/14
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/15
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/16
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/17
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/18
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/19
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/20
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/21
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/22
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/23
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/24
```

```
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/25
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/26
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/27
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/28
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/29
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/30
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/31
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/32
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/33
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/34
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/35
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/36
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/37
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/38
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/39
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/40
```

```
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/41
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/42
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/43
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/44
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/45
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/46
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/47
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/48
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/1/1
 shutdown
!
interface GigabitEthernet2/1/2
 shutdown
!
interface GigabitEthernet2/1/3
 shutdown
!
interface GigabitEthernet2/1/4
 shutdown
!
interface TenGigabitEthernet2/1/1
 shutdown
!
interface TenGigabitEthernet2/1/2
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan1000
 description Management VLAN for Switch
 ip address 10.10.127.11 255.255.255.0
!
ip default-gateway 10.10.127.1
ip classless
no ip forward-protocol nd
```

```
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication CiscoACS
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Vlan1000
!
!
ip sla enable reaction-alerts
logging trap debugging
logging source-interface Vlan1000
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFF0F
snmp-server trap-source Vlan1000
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps energywise
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps power-ethernet group 1-4
snmp-server enable traps power-ethernet police
snmp-server enable traps cpu threshold
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps errdisable
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
!
banner exec ^C
WARNING:
```

```
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication CiscoACS
 speed 115200
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
!
scheduler interval 500
ntp clock-period 36027426
ntp source Vlan1000
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end
```

```
S-A2-MED-1/2#
```

S-A2-MED-3

```
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
!
hostname S-A2-MED-3
!
boot-start-marker
boot-end-marker
!
logging buffered 50000
enable secret 5 <removed>
!

username bart privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
!
aaa new-model
!
!
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
system mtu routing 1500
no ip source-route
!
!
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
password encryption aes
!
crypto pki trustpoint TP-self-signed-1308417408
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1308417408
 revocation-check none
 rsakeypair TP-self-signed-1308417408
```

```
!
!
crypto pki certificate chain TP-self-signed-1308417408
 certificate self-signed 01
  <removed>  quit
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh version 2
ip scp server enable
!
!
interface FastEthernet0/1
 switchport access vlan 17
 shutdown
!
interface FastEthernet0/2
 switchport access vlan 17
 shutdown
!
interface FastEthernet0/3
 switchport access vlan 17
 shutdown
!
interface FastEthernet0/4
 switchport access vlan 17
 shutdown
!
interface FastEthernet0/5
 switchport access vlan 17
 shutdown
!
interface FastEthernet0/6
 switchport access vlan 17
 shutdown
!
interface FastEthernet0/7
 switchport access vlan 17
 shutdown
!
interface FastEthernet0/8
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/1
 shutdown
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
!
```

```
interface Vlan1000
 description Management VLAN for Switch
 ip address 10.10.127.13 255.255.255.0
!
ip default-gateway 10.10.127.1
ip classless
no ip forward-protocol nd
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication CiscoACS
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Vlan1000
!
!
ip sla enable reaction-alerts
logging trap debugging
logging source-interface Vlan1000
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFF0F
snmp-server trap-source Vlan1000
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps energywise
snmp-server enable traps entity
snmp-server enable traps power-ethernet group 1
snmp-server enable traps power-ethernet police
snmp-server enable traps cpu threshold
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps errdisable
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server host 192.168.42.124 remoteuser
```

```
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
banner exec ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^C
WARNING:
    *                   **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO ADMINISTRATOR OR OTHEMIME WITHOUT
FU L
NFORCEMENT OFFCIAL NDPRSETHO OF STATEAND FEER^C
banner login ^C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication CiscoACS
 speed 115200
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
!
ntp clock-period 36028775
ntp source Vlan1000
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end
```

Small Clinic

R-A2-SMALL

```
version 15.1
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
!
hostname R-A2-Small-1
!
boot-start-marker
boot system flash0 c2900-universalk9-mz.SPA.151-3.T.bin
boot-end-marker
!
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 50000
no logging rate-limit
enable secret 5 <removed>
!
aaa new-model
!
!
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
!
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PSTDST recurring
!
no ipv6 cef
ip source-route
ip cef
!
!
!
ip multicast-routing
!
!
no ip bootp server
ip domain name cisco-irn.com
ip name-server 192.168.42.130
ip port-map user-8443 port tcp 8443
ip ips notify SDEE
```

```
ip ips name COMPLIANCE-XXX
!
ip ips signature-category
  category all
   retired true
  category ios_ips default
   retired false
!
ip wccp 61
ip wccp 62
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
multilink bundle-name authenticated
!
parameter-map type inspect global
 WAAS enable
parameter-map type inspect Inspect-1
 audit-trail on

parameter-map type trend-global trend-glob-map
!
!
!
!
password encryption aes
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-503450500
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-503450500
 revocation-check none
 rsakeypair TP-self-signed-503450500
!
!
crypto pki certificate chain TP-self-signed-503450500
 certificate self-signed 01
  <removed>
    quit
voice-card 0
!
!
!
!
!
!
!
license udi pid CISCO2921/K9 sn <removed>
hw-module ism 0
!
hw-module sm 1
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
object-group network ActiveDirectory.cisco-irn.com
 host 192.168.42.130
!
```

```
object-group service CAPWAP
 description CAPWAP UDP ports 5246 and 5247
 udp eq 5246
 udp eq 5247
!
object-group service CISCO-WAAS
 description Ports for Cisco WAAS
 tcp eq 4050
!
object-group network DC-ALL
 description All of the Data Center
 192.168.0.0 255.255.0.0
!
object-group network Branches-ALL
 description all branch networks
 10.10.0.0 255.255.0.0
!
object-group network CSM_INLINE_dst_rule_68719541425
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
!
object-group network WCSManager
 description Wireless Manager
 host 192.168.43.135
!
object-group network DC-Wifi-Controllers
 description Central Wireless Controllers for branchs
 host 192.168.43.21
 host 192.168.43.22
!
object-group network DC-Wifi-MSE
 description Mobility Service Engines
 host 192.168.43.31
 host 192.168.43.32
!
object-group network CSM_INLINE_dst_rule_68719541431
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
!
object-group network PAME-DC-1
 host 192.168.44.111
!
object-group network MSP-DC-1
 description Data Center VSOM
 host 192.168.44.121
!
object-group network CSM_INLINE_dst_rule_68719541435
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object PAME-DC-1
 group-object MSP-DC-1
!
object-group network CSM_INLINE_dst_rule_68719541457
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
!
object-group network CSM_INLINE_dst_rule_68719541461
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
!
```

```
object-group network CSM_INLINE_dst_rule_68719541465
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
!
object-group network EMC-NCM
 description EMC Network Configuration Manager
 host 192.168.42.122
!
object-group network RSA-enVision
 description RSA EnVision Syslog collector and SIM
 host 192.168.42.124
!
object-group network CSM_INLINE_dst_rule_73014451187
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object EMC-NCM
 group-object RSA-enVision
!
object-group network TACACS
 description Csico Secure ACS server for TACACS and Radius
 host 192.168.42.131
!
object-group network RSA-AM
 description RSA Authentication Manager for SecureID
 host 192.168.42.137
!
object-group network NAC-1
 description ISE server for NAC
 host 192.168.42.111
!
object-group network CSM_INLINE_dst_rule_73014451193
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object ActiveDirectory.cisco-irn.com
 group-object TACACS
 group-object RSA-AM
 group-object NAC-1
!
object-group network NAC-2
 host 192.168.42.112
!
object-group network CSM_INLINE_dst_rule_73014451223
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object NAC-2
 group-object NAC-1
!
object-group network DC-Admin
 description DC Admin Systems
 host 192.168.41.101
 host 192.168.41.102
!
object-group network CSManager
 description Cisco Security Manager
 host 192.168.42.133
!
object-group network CSM_INLINE_src_rule_68719541409
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-Admin
 group-object EMC-NCM
 group-object CSManager
!
object-group network CSM_INLINE_src_rule_68719541427
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
```

```
!
object-group network CSM_INLINE_src_rule_68719541429
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
!
object-group network CSM_INLINE_src_rule_68719541433
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object PAME-DC-1
 group-object MSP-DC-1
!
object-group network DC-WAAS
 description WAE Appliances in Data Center
 host 192.168.48.10
 host 192.168.49.10
 host 192.168.47.11
 host 192.168.47.12
!
object-group network CSM_INLINE_src_rule_68719541437
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-Admin
 group-object DC-WAAS
!
object-group network DC-POS-Tomax
 description Tomax POS Communication from Store to Data Center
 192.168.52.96 255.255.255.224
!
object-group network DC-POS-SAP
 description SAP POS Communication from Store to Data Center
 192.168.52.144 255.255.255.240
!
object-group network DC-POS-Oracle
 description Oracle POS Communication from Store to Data Center
 192.168.52.128 255.255.255.240
!
object-group network CSM_INLINE_src_rule_73014451215
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-Admin
 group-object DC-POS-Tomax
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
!
object-group network CSM_INLINE_src_rule_73014451217
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-Admin
 group-object DC-POS-Tomax
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
!
object-group service CSM_INLINE_svc_rule_68719541409
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq 22
!
object-group service CSM_INLINE_svc_rule_68719541425
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
!
```

```
object-group service CSM_INLINE_svc_rule_68719541427
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
!
object-group service LWAPP
 description LWAPP UDP ports 12222 and 12223
 udp eq 12222
 udp eq 12223
!
object-group service TFTP
 description Trivial File Transfer
 tcp eq 69
 udp eq tftp
!
object-group service IP-Protocol-97
 description IP protocol 97
 97
!
object-group service CSM_INLINE_svc_rule_68719541429
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq www
 tcp eq 22
 tcp eq telnet
 udp eq isakmp
 group-object CAPWAP
 group-object LWAPP
 group-object TFTP
 group-object IP-Protocol-97
!
object-group service Cisco-Mobility
 description Mobility ports for Wireless
 udp eq 16666
 udp eq 16667
!
object-group service CSM_INLINE_svc_rule_68719541431
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 udp eq isakmp
 group-object CAPWAP
 group-object LWAPP
 group-object Cisco-Mobility
 group-object IP-Protocol-97
!
object-group service HTTPS-8443
 tcp eq 8443
!
object-group service Microsoft-DS-SMB
 description Microsoft-DS Active Directory, Windows shares Microsoft-DS SMB file sharing
 tcp eq 445
!
object-group service CSM_INLINE_svc_rule_68719541437
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp
 tcp eq 139
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Microsoft-DS-SMB
```

```
!
object-group service CSM_INLINE_svc_rule_68719541439
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp
 tcp eq 139
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_68719541455
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 icmp
 tcp-udp eq 5060
 tcp eq 2000
 tcp eq www
 tcp eq 443
 group-object TFTP
!
object-group service CSM_INLINE_svc_rule_68719541457
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp-udp eq 5060
 tcp eq 2000
!
object-group service Netbios
 description Netbios Servers
 udp eq netbios-dgm
 udp eq netbios-ns
 tcp eq 139
!
object-group service ORACLE-SIM
 description Oracle Store Inventory Management
 tcp eq 7777
 tcp eq 6003
 tcp range 12401 12500
!
object-group service RDP
 description Windows Remote Desktop
 tcp eq 3389
!
object-group service Workbrain
 tcp eq 8444
!
object-group service CSM_INLINE_svc_rule_68719541459
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq ftp
 tcp eq www
 tcp eq 443
 udp eq 88
 tcp-udp eq 42
 group-object Microsoft-DS-SMB
 group-object Netbios
 group-object ORACLE-SIM
 group-object RDP
 group-object Workbrain
!
object-group service CSM_INLINE_svc_rule_73014451187
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 udp eq syslog
 udp eq snmp
```

```
 udp eq snmptrap
!
object-group service CSM_INLINE_svc_rule_73014451193
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq tacacs
 udp eq 1812
 udp eq 1813
 tcp eq 389
 tcp eq 636
!
object-group service vCenter-to-ESX4
 description Communication from vCetner to ESX hosts
 tcp eq 5989
 tcp eq 8000
 tcp eq 902
 tcp eq 903
!
object-group service CSM_INLINE_svc_rule_73014451195
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq 22
 group-object vCenter-to-ESX4
!
object-group service ESX-SLP
 description CIM Service Location Protocol (SLP) for VMware systems
 udp eq 427
 tcp eq 427
!
object-group service CSM_INLINE_svc_rule_73014451197
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 group-object vCenter-to-ESX4
 group-object ESX-SLP
!
object-group service ORACLE-RMI
 description RMI TCP ports 1300 and 1301-1319.
 tcp range 1300 1319
!
object-group service ORACLE-Weblogic
 description HTTP/RMI and HTTPS/RMI-SSL 7001 & 7002. OracleAQ uses 1521.
 tcp eq 7001
 tcp eq 7002
 tcp eq 1521
!
object-group service ORACLE-WAS
 description RMI/IIOP over 2809  HTTP over 9443 IBM-MQ 1414
 tcp eq 2809
 tcp eq 9443
 tcp eq 1414
!
object-group service ORACLE-OAS
 description OAS uses one port for HTTP and RMI - 12601.
 tcp eq 12601
!
object-group service CSM_INLINE_svc_rule_73014451203
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq 22
 group-object ORACLE-RMI
```

```
 group-object ORACLE-Weblogic
 group-object ORACLE-WAS
 group-object ORACLE-OAS
!
object-group service CSM_INLINE_svc_rule_73014451205
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq 22
 group-object ORACLE-RMI
 group-object ORACLE-Weblogic
 group-object ORACLE-WAS
 group-object ORACLE-OAS
!
object-group service CSM_INLINE_svc_rule_73014451207
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq 22
 group-object HTTPS-8443
!
object-group service CSM_INLINE_svc_rule_73014451209
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq 22
 group-object HTTPS-8443
!
object-group service TOMAX-8990
 description Tomax Application Port
 tcp eq 8990
!
object-group service CSM_INLINE_svc_rule_73014451211
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 group-object TOMAX-8990
!
object-group service CSM_INLINE_svc_rule_73014451213
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 group-object TOMAX-8990
!
object-group service ICMP-Requests
 description ICMP requests
 icmp information-request
 icmp mask-request
 icmp timestamp-request
!
object-group service CSM_INLINE_svc_rule_73014451215
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
 icmp redirect
 icmp alternate-address
 group-object ICMP-Requests
!
object-group service CSM_INLINE_svc_rule_73014451217
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
```

```
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
 icmp redirect
 icmp alternate-address
 group-object ICMP-Requests
!
object-group service DNS-Resolving
 description Domain Name Server
 tcp eq domain
 udp eq domain
!
object-group service CSM_INLINE_svc_rule_73014451221
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 udp eq bootps
 group-object DNS-Resolving
!
object-group service CSM_INLINE_svc_rule_73014451223
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
 group-object HTTPS-8443
!
object-group service CSM_INLINE_svc_rule_73014451388
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp
 tcp eq 139
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_73014451393
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq smtp
 tcp eq pop3
 tcp eq 143
!
object-group service CSM_INLINE_svc_rule_73014451395
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_73014451397
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp
 udp
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_73014451404
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_73014451406
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
```

```
 tcp eq www
 tcp eq 443
 tcp eq smtp
 tcp eq pop3
 tcp eq 143
!
object-group network DC-Applications
 description Applications in the Data Center
 192.168.180.0 255.255.254.0
!
object-group network DC-Voice
 description Data Center Voice
 192.168.45.0 255.255.255.0
!
object-group network MS-Update
 description Windows Update Server
 host 192.168.42.150
!
object-group network MSExchange
 description Mail Server
 host 192.168.42.140
!
object-group service NTP
 description NTP Protocols
 tcp eq 123
 udp eq ntp
!
object-group network NTP-Servers
 description NTP Servers
 host 192.168.62.161
 host 162.168.62.162
!
object-group network POS-Store-SMALL-1
 description Small Store POS devices
 host 10.10.128.81
 host 10.10.128.82
!
object-group network BRANCH-POS
 group-object POS-Store-SMALL-1
!
object-group network vSphere-1
 description vSphere server for Lab
 host 192.168.41.102
!

username bart privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
redundancy
!
!
!
!
ip ssh version 2
ip scp server enable
!
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_7
 match protocol http
 match protocol https
 match protocol microsoft-ds
 match protocol ms-sql
 match protocol ms-sql-m
 match protocol netbios-dgm
```

```
 match protocol netbios-ns
 match protocol oracle
 match protocol oracle-em-vp
 match protocol oraclenames
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_10
 match access-group name CSM_ZBF_CMAP_ACL_10
 match class-map CSM_ZBF_CMAP_PLMAP_7
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_16
 match protocol http
 match protocol https
 match protocol isakmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_23
 match access-group name CSM_ZBF_CMAP_ACL_23
 match class-map CSM_ZBF_CMAP_PLMAP_16
class-map type inspect match-all CSM_ZBF_CLASS_MAP_32
 match access-group name CSM_ZBF_CMAP_ACL_32
class-map type inspect match-all CSM_ZBF_CLASS_MAP_11
 match access-group name CSM_ZBF_CMAP_ACL_11
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_5
 match protocol http
 match protocol https
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_22
 match access-group name CSM_ZBF_CMAP_ACL_22
 match class-map CSM_ZBF_CMAP_PLMAP_5
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_4
 match protocol http
 match protocol https
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_33
 match access-group name CSM_ZBF_CMAP_ACL_33
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_8
 match protocol sip
 match protocol sip-tls
 match protocol skinny
 match protocol tftp
 match protocol http
 match protocol https
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_12
 match access-group name CSM_ZBF_CMAP_ACL_12
 match class-map CSM_ZBF_CMAP_PLMAP_8
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_15
 match protocol http
 match protocol https
 match protocol netbios-ns
 match protocol netbios-dgm
 match protocol netbios-ssn
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_21
 match access-group name CSM_ZBF_CMAP_ACL_21
 match class-map CSM_ZBF_CMAP_PLMAP_15
```

```
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_17
 match protocol http
 match protocol https
 match protocol imap3
 match protocol pop3
 match protocol pop3s
 match protocol smtp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_30
 match access-group name CSM_ZBF_CMAP_ACL_30
 match class-map CSM_ZBF_CMAP_PLMAP_17
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_9
 match protocol syslog
 match protocol syslog-conn
 match protocol snmp
 match protocol snmptrap
class-map type inspect match-all CSM_ZBF_CLASS_MAP_13
 match access-group name CSM_ZBF_CMAP_ACL_13
 match class-map CSM_ZBF_CMAP_PLMAP_9
class-map type inspect match-all CSM_ZBF_CLASS_MAP_20
 match access-group name CSM_ZBF_CMAP_ACL_20
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_20
 match protocol http
 match protocol https
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
 match protocol ftp
 match protocol ssh
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_31
 match access-group name CSM_ZBF_CMAP_ACL_31
 match class-map CSM_ZBF_CMAP_PLMAP_20
class-map match-all BRANCH-BULK-DATA
 match protocol tftp
 match protocol nfs
 match access-group name BULK-DATA-APPS
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_10
 match protocol ldaps
 match protocol ldap
 match protocol ldap-admin
 match protocol radius
 match protocol tacacs
 match protocol tacacs-ds
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_14
 match access-group name CSM_ZBF_CMAP_ACL_14
 match class-map CSM_ZBF_CMAP_PLMAP_10
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_18
 match protocol http
 match protocol https
 match protocol udp
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_27
 match access-group name CSM_ZBF_CMAP_ACL_27
 match class-map CSM_ZBF_CMAP_PLMAP_18
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_22
 match protocol sip
 match protocol sip-tls
 match protocol skinny
 match protocol tcp
```

```
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_36
 match access-group name CSM_ZBF_CMAP_ACL_36
 match class-map CSM_ZBF_CMAP_PLMAP_22
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_11
 match protocol ntp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_15
 match access-group name CSM_ZBF_CMAP_ACL_15
 match class-map CSM_ZBF_CMAP_PLMAP_11
class-map type inspect match-all CSM_ZBF_CLASS_MAP_26
 match access-group name CSM_ZBF_CMAP_ACL_26
 match class-map CSM_ZBF_CMAP_PLMAP_17
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_12
 match protocol bootpc
 match protocol bootps
 match protocol udp
 match protocol tcp
 match protocol dns
 match protocol dhcp-failover
class-map type inspect match-all CSM_ZBF_CLASS_MAP_16
 match access-group name CSM_ZBF_CMAP_ACL_16
 match class-map CSM_ZBF_CMAP_PLMAP_12
class-map type inspect match-all CSM_ZBF_CLASS_MAP_25
 match access-group name CSM_ZBF_CMAP_ACL_25
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_34
 match access-group name CSM_ZBF_CMAP_ACL_34
class-map type inspect match-all CSM_ZBF_CLASS_MAP_17
 match access-group name CSM_ZBF_CMAP_ACL_17
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_24
 match access-group name CSM_ZBF_CMAP_ACL_24
 match class-map CSM_ZBF_CMAP_PLMAP_7
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_21
 match protocol tcp
 match protocol udp
 match protocol http
 match protocol https
class-map type inspect match-all CSM_ZBF_CLASS_MAP_35
 match access-group name CSM_ZBF_CMAP_ACL_35
 match class-map CSM_ZBF_CMAP_PLMAP_21
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_13
 match protocol https
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_18
 match access-group name CSM_ZBF_CMAP_ACL_18
 match class-map CSM_ZBF_CMAP_PLMAP_13
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_14
 match protocol http
 match protocol https
 match protocol user-8443
class-map type inspect match-all CSM_ZBF_CLASS_MAP_19
 match access-group name CSM_ZBF_CMAP_ACL_19
 match class-map CSM_ZBF_CMAP_PLMAP_14
class-map type inspect match-all CSM_ZBF_CLASS_MAP_29
 match access-group name CSM_ZBF_CMAP_ACL_29
 match class-map CSM_ZBF_CMAP_PLMAP_18
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_19
 match protocol http
 match protocol https
 match protocol icmp
 match protocol tcp
```

```
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_28
 match access-group name CSM_ZBF_CMAP_ACL_28
 match class-map CSM_ZBF_CMAP_PLMAP_19
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_1
 match protocol https
 match protocol ssh
class-map type inspect match-all CSM_ZBF_CLASS_MAP_1
 match access-group name CSM_ZBF_CMAP_ACL_1
 match class-map CSM_ZBF_CMAP_PLMAP_1
class-map type inspect match-all CSM_ZBF_CLASS_MAP_3
 match access-group name CSM_ZBF_CMAP_ACL_3
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_2
 match protocol https
 match protocol http
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_2
 match access-group name CSM_ZBF_CMAP_ACL_2
 match class-map CSM_ZBF_CMAP_PLMAP_2
class-map type inspect match-all CSM_ZBF_CLASS_MAP_5
 match access-group name CSM_ZBF_CMAP_ACL_5
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_3
 match protocol http
 match protocol https
 match protocol ssh
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_4
 match access-group name CSM_ZBF_CMAP_ACL_4
 match class-map CSM_ZBF_CMAP_PLMAP_3
class-map type inspect match-all CSM_ZBF_CLASS_MAP_7
 match access-group name CSM_ZBF_CMAP_ACL_7
 match class-map CSM_ZBF_CMAP_PLMAP_5
class-map type inspect match-all CSM_ZBF_CLASS_MAP_6
 match access-group name CSM_ZBF_CMAP_ACL_6
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_9
 match access-group name CSM_ZBF_CMAP_ACL_9
 match protocol tcp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_6
 match protocol http
 match protocol https
 match protocol ssh
 match protocol telnet
 match protocol tftp
 match protocol isakmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_8
 match access-group name CSM_ZBF_CMAP_ACL_8
 match class-map CSM_ZBF_CMAP_PLMAP_6
class-map match-all BULK-DATA
 match ip dscp af11  af12
class-map match-all INTERACTIVE-VIDEO
 match ip dscp af41  af42
class-map match-any BRANCH-TRANSACTIONAL-DATA
 match protocol citrix
 match protocol ldap
 match protocol telnet
 match protocol sqlnet
 match protocol http url "*SalesReport*"
 match access-group name TRANSACTIONAL-DATA-APPS
```

```
class-map match-all BRANCH-MISSION-CRITICAL
 match access-group name MISSION-CRITICAL-SERVERS
class-map match-all VOICE
 match ip dscp ef
class-map match-all MISSION-CRITICAL-DATA
 match ip dscp 25
class-map match-any BRANCH-NET-MGMT
 match protocol snmp
 match protocol syslog
 match protocol dns
 match protocol icmp
 match protocol ssh
 match access-group name NET-MGMT-APPS
class-map match-all ROUTING
 match ip dscp cs6
class-map match-all SCAVENGER
 match ip dscp cs1
class-map match-all NET-MGMT
 match ip dscp cs2
class-map match-any BRANCH-SCAVENGER
 match protocol gnutella
 match protocol fasttrack
 match protocol kazaa2
class-map match-any CALL-SIGNALING
 match ip dscp cs3
class-map match-all TRANSACTIONAL-DATA
 match ip dscp af21  af22
!
!
policy-map BRANCH-LAN-EDGE-OUT
 class class-default
policy-map BRANCH-WAN-EDGE
 class VOICE
  priority percent 18
 class INTERACTIVE-VIDEO
  priority percent 15
 class CALL-SIGNALING
  bandwidth percent 5
 class ROUTING
  bandwidth percent 3
 class NET-MGMT
  bandwidth percent 2
 class MISSION-CRITICAL-DATA
  bandwidth percent 15
  random-detect
 class TRANSACTIONAL-DATA
  bandwidth percent 12
  random-detect dscp-based
 class BULK-DATA
  bandwidth percent 4
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 1
 class class-default
  bandwidth percent 25
  random-detect
policy-map type inspect CSM_ZBF_POLICY_MAP_18
 class type inspect CSM_ZBF_CLASS_MAP_28
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_19
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
```

```
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_29
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_30
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_31
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_16
 class type inspect CSM_ZBF_CLASS_MAP_24
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_25
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_26
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_27
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_17
 class type inspect CSM_ZBF_CLASS_MAP_25
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_26
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_27
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_14
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_15
 class type inspect CSM_ZBF_CLASS_MAP_13
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_23
  inspect Inspect-1
```

```
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_12
 class type inspect CSM_ZBF_CLASS_MAP_13
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_21
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_30
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_34
  drop log
 class type inspect CSM_ZBF_CLASS_MAP_35
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_13
 class type inspect CSM_ZBF_CLASS_MAP_13
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_21
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_20
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_32
  drop log
 class type inspect CSM_ZBF_CLASS_MAP_33
  inspect Inspect-1
```

```
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_10
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_11
 class type inspect CSM_ZBF_CLASS_MAP_13
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_22
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_36
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_9
 class type inspect CSM_ZBF_CLASS_MAP_13
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_8
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_12
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_7
 class type inspect CSM_ZBF_CLASS_MAP_9
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_10
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_11
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_6
 class type inspect CSM_ZBF_CLASS_MAP_6
```

```
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_5
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_8
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_4
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_7
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_3
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_5
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_2
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_4
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_1
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_2
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop
policy-map BRANCH-LAN-EDGE-IN
 class BRANCH-MISSION-CRITICAL
  set ip dscp 25
 class BRANCH-TRANSACTIONAL-DATA
  set ip dscp af21
 class BRANCH-NET-MGMT
  set ip dscp cs2
 class BRANCH-BULK-DATA
  set ip dscp af11
 class BRANCH-SCAVENGER
  set ip dscp cs1
!
```

```
zone security S_WAN
 description Store WAN Link
zone security LOOPBACK
 description Loopback interface
zone security S_MGMT
 description VLAN1000 Management
zone security S_Security
 description VLAN20 Physical Security Systems
zone security S_WAAS
 description VLAN19 WAAS optimization
zone security S_WLC-AP
 description VLAN18 Wireless Systems
zone security S_Data
 description VLAN12 Store Data
zone security S_Data-W
 description VLAN14 Store Wireless Data
zone security S_Guest
 description VLAN17 Guest/Public Wireless
zone security S_Voice
 description VLAN13 Store Voice
zone security S_Partners
 description VLAN16 Partner network
zone security S_POS
 description VLAN 11 POS Data
zone security S_POS-W
 description VLAN15 Store Wireless POS
zone security S_HIPAA
 description VLAN21 HIPAA
zone security S_HIPAA-WU
 description VLAN15 Wireless HIPAA Users
zone security S_HIPAA-WD
 description VLAN15 Wireless HIPAA Devices
zone-pair security CSM_S_WAN-LOOPBACK_1 source S_WAN destination LOOPBACK
 service-policy type inspect CSM_ZBF_POLICY_MAP_1
zone-pair security CSM_S_WAN-S_MGMT_1 source S_WAN destination S_MGMT
 service-policy type inspect CSM_ZBF_POLICY_MAP_2
zone-pair security CSM_S_WAN-S_Security_1 source S_WAN destination S_Security
 service-policy type inspect CSM_ZBF_POLICY_MAP_3
zone-pair security CSM_S_WAN-S_WAAS_1 source S_WAN destination S_WAAS
 service-policy type inspect CSM_ZBF_POLICY_MAP_4
zone-pair security CSM_S_WAN-S_WLC-AP_1 source S_WAN destination S_WLC-AP
 service-policy type inspect CSM_ZBF_POLICY_MAP_5
zone-pair security CSM_S_WAN-S_Data_1 source S_WAN destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Data-W_1 source S_WAN destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Guest_1 source S_WAN destination S_Guest
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Partners_1 source S_WAN destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_POS_1 source S_WAN destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_POS-W_1 source S_WAN destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_HIPAA_1 source S_WAN destination S_HIPAA
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_HIPAA-WU_1 source S_WAN destination S_HIPAA-WU
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_Voice_1 source S_WAN destination S_Voice
 service-policy type inspect CSM_ZBF_POLICY_MAP_8
zone-pair security CSM_LOOPBACK-S_WAN_1 source LOOPBACK destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_9
zone-pair security CSM_LOOPBACK-S_POS_1 source LOOPBACK destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
```

```
zone-pair security CSM_LOOPBACK-S_POS-W_1 source LOOPBACK destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_MGMT-S_WAN_1 source S_MGMT destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_11
zone-pair security CSM_S_MGMT-S_POS_1 source S_MGMT destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_MGMT-S_POS-W_1 source S_MGMT destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_Security-S_WAN_1 source S_Security destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_12
zone-pair security CSM_S_Security-S_POS_1 source S_Security destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_Security-S_POS-W_1 source S_Security destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_WAAS-S_WAN_1 source S_WAAS destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_13
zone-pair security CSM_S_WAAS-S_POS_1 source S_WAAS destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_WAAS-S_POS-W_1 source S_WAAS destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_WAAS-S_Data_1 source S_WAAS destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_Data-W_1 source S_WAAS destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_Partners_1 source S_WAAS destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WLC-AP-S_WAN_1 source S_WLC-AP destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_15
zone-pair security CSM_S_WLC-AP-S_POS_1 source S_WLC-AP destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_WLC-AP-S_POS-W_1 source S_WLC-AP destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_POS-S_WAN_1 source S_POS destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_16
zone-pair security CSM_S_POS-W-S_WAN_1 source S_POS-W destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_17
zone-pair security CSM_S_POS-W-S_POS_1 source S_POS-W destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
zone-pair security CSM_S_Data-S_POS_1 source S_Data destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_Data-S_POS-W_1 source S_Data destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_Data-S_WAN_1 source S_Data destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_19
zone-pair security CSM_S_Data-W-S_POS_1 source S_Data-W destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_Data-W-S_POS-W_1 source S_Data-W destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_Data-W-S_WAN_1 source S_Data-W destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_19
zone-pair security CSM_S_Guest-S_POS_1 source S_Guest destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_Guest-S_POS-W_1 source S_Guest destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_Guest-S_WAN_1 source S_Guest destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_20
zone-pair security CSM_S_Partners-S_POS_1 source S_Partners destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_Partners-S_POS-W_1 source S_Partners destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_Partners-S_WAN_1 source S_Partners destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_21
zone-pair security CSM_S_Voice-S_POS_1 source S_Voice destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
```

```
zone-pair security CSM_S_Voice-S_POS-W_1 source S_Voice destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_Voice-S_WAN_1 source S_Voice destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_22
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.10.142.1 255.255.255.255
 ip pim sparse-dense-mode
 zone-member security LOOPBACK
!
interface GigabitEthernet0/0
 description ROUTER LINK TO SWITCH
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.11
 description POS
 encapsulation dot1Q 11
 ip address 10.10.128.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_POS
 standby 11 ip 10.10.128.1
 standby 11 priority 101
 standby 11 preempt
 ip igmp query-interval 125
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.12
 description DATA
 encapsulation dot1Q 12
 ip address 10.10.129.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip wccp 61 redirect in
 ip pim sparse-dense-mode
 zone-member security S_Data
 standby 12 ip 10.10.129.1
 standby 12 priority 101
 standby 12 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.13
 description VOICE
 encapsulation dot1Q 13
 ip address 10.10.130.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_Voice
 standby 13 ip 10.10.130.1
 standby 13 priority 101
 standby 13 preempt
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.14
 description WIRELESS
```

```
 encapsulation dot1Q 14
 ip address 10.10.131.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Data-W
 standby 14 ip 10.10.131.1
 standby 14 priority 101
 standby 14 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.15
 description WIRELESS-POS
 encapsulation dot1Q 15
 ip address 10.10.132.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_POS-W
 standby 15 ip 10.10.132.1
 standby 15 priority 101
 standby 15 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.16
 description PARTNER
 encapsulation dot1Q 16
 ip address 10.10.133.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Partners
 standby 16 ip 10.10.133.1
 standby 16 priority 101
 standby 16 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.17
 description WIRELESS-GUEST
 encapsulation dot1Q 17
 ip address 10.10.134.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Guest
 standby 17 ip 10.10.134.1
 standby 17 priority 101
 standby 17 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.18
 description WIRELESS-CONTROL
 encapsulation dot1Q 18
 ip address 10.10.135.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_WLC-AP
 standby 18 ip 10.10.135.1
 standby 18 priority 101
 standby 18 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.19
 description WAAS
 encapsulation dot1Q 19
 ip address 10.10.136.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_WAAS
```

```
 standby 19 ip 10.10.136.1
 standby 19 priority 101
 standby 19 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.20
 description SECURITY-SYSTEMS
 encapsulation dot1Q 20
 ip address 10.10.137.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_Security
 standby 20 ip 10.10.137.1
 standby 20 priority 101
 standby 20 preempt
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.21
 description HIPAA
 encapsulation dot1Q 21
 ip address 10.10.138.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_HIPAA
 standby 21 ip 10.10.138.1
 standby 21 priority 101
 standby 21 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.22
 description WIRELESS-HIPAA-USERS
 encapsulation dot1Q 22
 ip address 10.10.139.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_HIPAA-WU
 standby 22 ip 10.10.139.1
 standby 22 priority 101
 standby 22 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.23
 description WIRELESS-HIPAA-DEVICES
 encapsulation dot1Q 23
 ip address 10.10.140.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_HIPAA-WD
 standby 23 ip 10.10.140.1
 standby 23 priority 101
 standby 23 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/0.1000
 description MANAGEMENT
 encapsulation dot1Q 1000
 ip address 10.10.143.2 255.255.255.0
 zone-member security S_MGMT
 standby 100 ip 10.10.143.1
 standby 100 priority 101
```

```
 standby 100 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface ISM0/0
 no ip address
 shutdown
 !Application: Online on SME
 hold-queue 60 out
!
interface GigabitEthernet0/1
 ip address 10.10.255.128 255.255.255.0
 ip ips COMPLIANCE-XXX in
 zone-member security S_WAN
 duplex auto
 speed auto
 service-policy output BRANCH-WAN-EDGE
!
interface GigabitEthernet0/2
 ip address 10.10.254.128 255.255.255.0
 ip ips COMPLIANCE-XXX in
 zone-member security S_WAN
 duplex auto
 speed auto
 service-policy output BRANCH-WAN-EDGE
!
interface ISM0/1
 description Internal switch interface connected to Internal Service Module
 shutdown
!
interface SM1/0
 no ip address
 zone-member security S_Security
 shutdown
 service-module fail-open
 hold-queue 60 out
!
interface SM1/1
 description Internal switch interface connected to Service Module
!
interface Vlan1
 no ip address
 zone-member security S_POS
!
!
router ospf 5
 router-id 10.10.142.1
 passive-interface default
!
no ip forward-protocol nd
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication CiscoACS
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip route 0.0.0.0 0.0.0.0 10.10.255.11
ip route 0.0.0.0 0.0.0.0 10.10.254.11 50
ip tacacs source-interface Loopback0
!
ip access-list extended BULK-DATA-APPS
 remark ---File Transfer---
```

```
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
 remark ---E-mail traffic---
 permit tcp any any eq smtp
 permit tcp any any eq pop3
 permit tcp any any eq 143
 remark ---other EDM app protocols---
 permit tcp any any range 3460 3466
 permit tcp any range 3460 3466 any
 remark ---messaging services---
 permit tcp any any eq 2980
 permit tcp any eq 2980 any
 remark ---Microsoft file services---
 permit tcp any any range 137 139
 permit tcp any range 137 139 any
ip access-list extended CSM_ZBF_CMAP_ACL_1
 remark Data Center Mgmt to Devices
 permit object-group CSM_INLINE_svc_rule_68719541409 object-group
CSM_INLINE_src_rule_68719541409 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_10
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451205 object-group DC-POS-Oracle
object-group BRANCH-POS
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451209 object-group DC-POS-SAP object-group
BRANCH-POS
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451213 object-group DC-POS-Tomax
object-group BRANCH-POS
ip access-list extended CSM_ZBF_CMAP_ACL_11
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451215 object-group
CSM_INLINE_src_rule_73014451215 object-group BRANCH-POS
ip access-list extended CSM_ZBF_CMAP_ACL_12
 remark Data Center VOICE (wired and Wireless)
 permit object-group CSM_INLINE_svc_rule_68719541455 object-group DC-Voice object-group
Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_13
 remark Syslog and SNMP Alerts
 permit object-group CSM_INLINE_svc_rule_73014451187 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_73014451187
ip access-list extended CSM_ZBF_CMAP_ACL_14
 remark Store to Data Center Authentications
 permit object-group CSM_INLINE_svc_rule_73014451193 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_73014451193
ip access-list extended CSM_ZBF_CMAP_ACL_15
 remark Store to Data Center for NTP
 permit object-group NTP object-group Branches-ALL object-group NTP-Servers
ip access-list extended CSM_ZBF_CMAP_ACL_16
 remark Store to Data Center for DHCP and DNS
 permit object-group CSM_INLINE_svc_rule_73014451221 object-group Branches-ALL
object-group ActiveDirectory.cisco-irn.com
ip access-list extended CSM_ZBF_CMAP_ACL_17
 remark Permit ICMP traffic
 permit object-group CSM_INLINE_svc_rule_68719541425 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_68719541425
ip access-list extended CSM_ZBF_CMAP_ACL_18
 remark Store UCS E-series server to Data Center vShphere
 permit object-group CSM_INLINE_svc_rule_73014451197 object-group Branches-ALL
object-group vSphere-1
ip access-list extended CSM_ZBF_CMAP_ACL_19
 remark Store NAC
 permit object-group CSM_INLINE_svc_rule_73014451223 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_73014451223
```

```
ip access-list extended CSM_ZBF_CMAP_ACL_2
 remark Data Center subscribe to IPS SDEE events
 permit tcp object-group RSA-enVision object-group Branches-ALL eq 443
ip access-list extended CSM_ZBF_CMAP_ACL_20
 remark Store to Data Center Physical Security
 permit ip object-group Branches-ALL object-group CSM_INLINE_dst_rule_68719541435
ip access-list extended CSM_ZBF_CMAP_ACL_21
 remark Store WAAS (WAAS Devices need their own zone)
 permit object-group CSM_INLINE_svc_rule_68719541439 object-group Branches-ALL
object-group DC-WAAS
ip access-list extended CSM_ZBF_CMAP_ACL_22
 remark Store WAAS to Clients and Servers
 permit object-group CSM_INLINE_svc_rule_73014451388 object-group Branches-ALL
object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_23
 remark Store to Data Center wireless controller traffic
 permit object-group CSM_INLINE_svc_rule_68719541431 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_68719541431
ip access-list extended CSM_ZBF_CMAP_ACL_24
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451203 object-group BRANCH-POS object-group
DC-POS-Oracle
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451207 object-group BRANCH-POS object-group
DC-POS-SAP
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451211 object-group BRANCH-POS object-group
DC-POS-Tomax
ip access-list extended CSM_ZBF_CMAP_ACL_25
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451217 object-group
CSM_INLINE_src_rule_73014451217 object-group BRANCH-POS
ip access-list extended CSM_ZBF_CMAP_ACL_26
 remark Store to Data Center for E-mail
 permit object-group CSM_INLINE_svc_rule_73014451393 object-group BRANCH-POS object-group
MSExchange
ip access-list extended CSM_ZBF_CMAP_ACL_27
 remark Store to Data Center for Windows Updates
 permit object-group CSM_INLINE_svc_rule_73014451395 object-group BRANCH-POS object-group
MS-Update
ip access-list extended CSM_ZBF_CMAP_ACL_28
 remark Permit POS clients to talk to branch POS server
 permit object-group CSM_INLINE_svc_rule_73014451397 object-group BRANCH-POS object-group
BRANCH-POS
ip access-list extended CSM_ZBF_CMAP_ACL_29
 remark Store to Data Center for Windows Updates
 permit object-group CSM_INLINE_svc_rule_73014451404 object-group Branches-ALL
object-group MS-Update
ip access-list extended CSM_ZBF_CMAP_ACL_3
 remark Permit ICMP traffic
 permit object-group CSM_INLINE_svc_rule_68719541427 object-group
CSM_INLINE_src_rule_68719541427 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_30
 remark Store to Data Center for E-mail
 permit object-group CSM_INLINE_svc_rule_73014451406 object-group Branches-ALL
object-group MSExchange
ip access-list extended CSM_ZBF_CMAP_ACL_31
 remark Store DATA (wired and Wireless - Access to DC Other applications)
 permit object-group CSM_INLINE_svc_rule_68719541459 object-group Branches-ALL
object-group DC-Applications
ip access-list extended CSM_ZBF_CMAP_ACL_32
 remark Store GUEST - Drop Traffic to Enterprise
 permit ip object-group Branches-ALL object-group CSM_INLINE_dst_rule_68719541465
ip access-list extended CSM_ZBF_CMAP_ACL_33
```

```
 remark Store GUEST (access to internet/DMZ web servers)
 permit ip object-group Branches-ALL any
ip access-list extended CSM_ZBF_CMAP_ACL_34
 remark Store PARTNERS - Drop Traffic to Enterprise
 permit ip object-group Branches-ALL object-group CSM_INLINE_dst_rule_68719541461
ip access-list extended CSM_ZBF_CMAP_ACL_35
 remark Store PARTNERS (wired and wireless - Access to Partner site, Internet VPN)
 permit ip object-group Branches-ALL any
ip access-list extended CSM_ZBF_CMAP_ACL_36
 remark Store VOICE (wired and Wireless - Acess to corporate wide voice)
 permit object-group CSM_INLINE_svc_rule_68719541457 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_68719541457
ip access-list extended CSM_ZBF_CMAP_ACL_4
 remark Data Center vSphere to UCS E-series server
 permit object-group CSM_INLINE_svc_rule_73014451195 object-group vSphere-1 object-group
Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_5
 remark Data Center to Store Physical Security
 permit ip object-group CSM_INLINE_src_rule_68719541433 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_6
 remark Data Center Mgmt to Devices
 permit object-group RDP object-group DC-Admin object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_7
 remark Data Center WAAS to Store
 permit object-group CSM_INLINE_svc_rule_68719541437 object-group
CSM_INLINE_src_rule_68719541437 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_8
 remark Data Center Wireless Control to AP's and Controllers in branchs
 permit object-group CSM_INLINE_svc_rule_68719541429 object-group
CSM_INLINE_src_rule_68719541429 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_9
 remark Data Center Mgmt to Devices
 permit object-group RDP object-group DC-Admin object-group BRANCH-POS
ip access-list extended MISSION-CRITICAL-SERVERS
 remark ---POS Applications---
 permit ip any 192.168.52.0 0.0.0.255
ip access-list extended NET-MGMT-APPS
 remark - Router user Authentication - Identifies TACACS Control traffic
 permit tcp any any eq tacacs
 permit tcp any eq tacacs any
ip access-list extended TRANSACTIONAL-DATA-APPS
 remark ---Workbrain Application---
 remark --Large Store Clock Server to Central Clock Application
 permit tcp host 10.10.49.94 host 192.168.46.72 eq 8444
 remark --Large branch Clock Server to CUAE
 permit tcp host 10.10.49.94 host 192.168.45.185 eq 8000
 remark ---LiteScape Application---
 permit ip any host 192.168.46.82
 permit ip any 239.192.0.0 0.0.0.255
 permit ip any host 239.255.255.250
 remark ---Remote Desktop---
 permit tcp any any eq 3389
 permit tcp any eq 3389 any
 remark ---Oracle SIM---
 permit tcp any 192.168.46.0 0.0.0.255 eq 7777
 permit tcp any 192.168.46.0 0.0.0.255 eq 6003
 permit tcp any 192.168.46.0 0.0.0.255 range 12401 12500
 permit tcp 192.168.46.0 0.0.0.255 eq 7777 any
 permit tcp 192.168.46.0 0.0.0.255 eq 6003 any
 permit tcp 192.168.46.0 0.0.0.255 range 12401 12500 any
!
logging esm config
logging trap debugging
logging source-interface Loopback0
```

```
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
!
!
!
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps flash insertion removal
snmp-server enable traps energywise
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps ipsla
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server domain-stripping
tacacs-server key 7 <removed>
!
!
control-plane
!
!
!
!
mgcp profile default
!
!
!
!
!
gatekeeper
 shutdown
!
!
banner exec C
```

```
WARNING:
**** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
**** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner incoming C
WARNING:
**** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
**** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner login C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!


!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication CiscoACS
line aux 0
 session-timeout 1  output
 exec-timeout 0 1
 privilege level 0
 no exec
 transport preferred none
 transport output none
line 67
 no activation-character
 no exec
 transport preferred none
 transport input ssh
 transport output none
 stopbits 1
 flowcontrol software
line 131
 no activation-character
 no exec
 transport preferred none
 transport input ssh
 transport output none
 stopbits 1
 flowcontrol software
line vty 0 4
 session-timeout 15  output
```

```
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162
end
```

S-A2-SMALL

```
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
!
hostname S-A2-Small-1
!
boot-start-marker
boot-end-marker
!
logging buffered 50000
enable secret 5 <removed>
!

username bart privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
!
aaa new-model
!
!
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
```

```
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
switch 1 provision ws-c2960s-48fps-l
switch 2 provision ws-c2960s-48fps-l
authentication mac-move permit
ip subnet-zero
no ip source-route
!
!
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
password encryption aes
!
crypto pki trustpoint TP-self-signed-1383908352
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1383908352
 revocation-check none
 rsakeypair TP-self-signed-1383908352
!
!
crypto pki certificate chain TP-self-signed-1383908352
 certificate self-signed 01
  30820252 308201BB A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 31333833 39303833 3532301E 170D3131 30343232 30333331
  35375A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 33383339
  30383335 3230819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100BD50 C6915FE3 A1789C0E 11A0BABD EC2528DB 3F8FBCF6 64D90C72 AD2D2A13
  A012AB72 F5F9EEDE 4E77EDA9 D3CE6985 BA2246A1 21FF6D61 B8FFC558 331CD608
  DB59F546 838396C6 29266AF9 6B968127 75A7CE55 6D0B3734 0454EA42 24E9C995
  1AC5D0C3 0850D703 F58A2E82 6FB13D8D 372F03D8 A5B2B577 CDB7A9D5 7AFC40B6
  B26B0203 010001A3 7A307830 0F060355 1D130101 FF040530 030101FF 30250603
  551D1104 1E301C82 1A532D41 322D536D 616C6C2D 312E6369 73636F2D 69726E2E
  636F6D30 1F060355 1D230418 30168014 107F4DD8 762989FE 887F813D 62A1D871
  C9A4D3D4 301D0603 551D0E04 16041410 7F4DD876 2989FE88 7F813D62 A1D871C9
  A4D3D430 0D06092A 864886F7 0D010104 05000381 810045BF 884709EE FA837D06
  262E65C8 865912B1 44D5DE7F 459A7DEF DAEB3D94 B2D5A978 5CCF425E 1FED41CE
  2046BA9D 130DE1BD 4A7F3F99 B6AD32CA 3857A088 01083AAB 24557476 73F8AAC6
  634964A5 455F4DB2 AC36D64E EA2C71AD 296D82B6 CE1EDCCB 0724DB5D 0D332C10
  A17D5B1F E8926DC9 137519A1 521C9155 AF9AF52B 00BD
  quit
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
spanning-tree mode pvst
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
ip ssh time-out 30
ip ssh authentication-retries 2
```

```
ip ssh version 2
ip scp server enable
!
!
interface FastEthernet0
 no ip address
!
interface GigabitEthernet1/0/1
 switchport mode trunk
!
interface GigabitEthernet1/0/2
 switchport mode trunk
!
interface GigabitEthernet1/0/3
 description IP Cameras - 4300
 switchport access vlan 20
 switchport mode access
!
interface GigabitEthernet1/0/4
 description CPAM Gateway
 switchport access vlan 20
!
interface GigabitEthernet1/0/5
 switchport mode trunk
!
interface GigabitEthernet1/0/6
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/7
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/8
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/9
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/10
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/11
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/12
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/13
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/14
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/15
 switchport access vlan 17
 shutdown
```

```
!
interface GigabitEthernet1/0/16
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/17
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/18
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/19
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/20
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/21
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/22
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/23
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/24
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/25
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/26
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/27
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/28
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/29
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/30
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/31
 switchport access vlan 17
 shutdown
```

```
!
interface GigabitEthernet1/0/32
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/33
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/34
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/35
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/36
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/37
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/38
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/39
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/40
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/41
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/42
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/43
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/44
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/45
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/46
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/47
 switchport access vlan 17
 shutdown
```

```
!
interface GigabitEthernet1/0/48
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/49
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/50
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/51
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet1/0/52
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/1
 shutdown
!
interface GigabitEthernet2/0/2
 shutdown
!
interface GigabitEthernet2/0/3
 description Cisco7975 IP phone
 switchport access vlan 11
 switchport voice vlan 13
 spanning-tree portfast
!
interface GigabitEthernet2/0/4
 description AIR-CAP3502I
 switchport trunk native vlan 18
 switchport trunk allowed vlan 14-18
 switchport mode trunk
!
interface GigabitEthernet2/0/5
 description Cisco9971 IP phone
 switchport access vlan 11
 switchport voice vlan 13
 spanning-tree portfast
!
interface GigabitEthernet2/0/6
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/7
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/8
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/9
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/10
 switchport access vlan 17
 shutdown
```

```
!
interface GigabitEthernet2/0/11
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/12
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/13
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/14
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/15
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/16
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/17
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/18
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/19
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/20
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/21
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/22
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/23
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/24
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/25
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/26
 switchport access vlan 17
 shutdown
```

```
!
interface GigabitEthernet2/0/27
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/28
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/29
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/30
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/31
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/32
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/33
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/34
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/35
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/36
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/37
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/38
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/39
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/40
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/41
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/42
 switchport access vlan 17
 shutdown
```

```
!
interface GigabitEthernet2/0/43
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/44
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/45
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/46
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/47
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/48
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/49
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/50
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/51
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet2/0/52
 switchport access vlan 17
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan1000
 description Management VLAN for Switch
 ip address 10.10.143.11 255.255.255.0
!
ip default-gateway 10.10.143.1
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication CiscoACS
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Vlan1000
!
ip sla enable reaction-alerts
logging trap debugging
logging source-interface Vlan1000
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
```

```
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFF0F
snmp-server trap-source Vlan1000
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps energywise
snmp-server enable traps entity
snmp-server enable traps power-ethernet group 1-4
snmp-server enable traps power-ethernet police
snmp-server enable traps cpu threshold
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps errdisable
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
!
banner exec ^CC
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^CC
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****
ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
```

```
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^CC
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication CiscoACS
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
!
ntp clock-period 22518357
ntp source Vlan1000
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end
```

Mini Clinic

R-A2-MINI-1

```
version 15.1
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
!
hostname R-A2-Mini-1
!
boot-start-marker
```

```
boot system flash0 c1900-universalk9-mz.SPA.151-3.T.bin
boot-end-marker
!
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 50000
no logging rate-limit
enable secret 5 <removed>
!
aaa new-model
!
!
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default
 action-type start-stop
 group tacacs+
!
aaa accounting commands 15 default
 action-type start-stop
 group tacacs+
!
aaa accounting system default
 action-type start-stop
 group tacacs+
!
!
!
!
!
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PST recurring
service-module wlan-ap 0 bootimage autonomous
!
no ipv6 cef
no ip source-route
ip cef
!
!
!
ip multicast-routing
!
!
no ip bootp server
ip domain name cisco-irn.com
ip name-server 192.168.42.130
ip port-map user-8443 port tcp 8443
ip inspect log drop-pkt
ip inspect audit-trail
ip ips config location flash0: retries 1 timeout 1
ip ips notify SDEE
ip ips name Store-IPS
!
ip ips signature-category
  category all
   retired true
  category ios_ips default
   retired false
```

```
!
ip wccp 61
ip wccp 62
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
multilink bundle-name authenticated
!
parameter-map type inspect Inspect-1
 audit-trail on
parameter-map type inspect global
 WAAS enable

parameter-map type trend-global trend-glob-map
password encryption aes
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-1721465088
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1721465088
 revocation-check none
 rsakeypair TP-self-signed-1721465088
!
!
crypto pki certificate chain TP-self-signed-1721465088
 certificate self-signed 01
  <removed>
    quit
license udi pid CISCO1941W-A/K9 sn <removed>
hw-module ism 0
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
object-group network ActiveDirectory.cisco-irn.com
 host 192.168.42.130
!
object-group service CAPWAP
 description CAPWAP UDP ports 5246 and 5247
 udp eq 5246
 udp eq 5247
!
object-group service CISCO-WAAS
 description Ports for Cisco WAAS
 tcp eq 4050
!
object-group network DC-ALL
 description All of the Data Center
 192.168.0.0 255.255.0.0
!
object-group network Branches-ALL
 description all branch networks
 10.10.0.0 255.255.0.0
!
object-group network CSM_INLINE_dst_rule_68719541425
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
```

```
!
object-group network WCSManager
 description Wireless Manager
 host 192.168.43.135
!
object-group network DC-Wifi-Controllers
 description Central Wireless Controllers for branchs
 host 192.168.43.21
 host 192.168.43.22
!
object-group network DC-Wifi-MSE
 description Mobility Service Engines
 host 192.168.43.31
 host 192.168.43.32
!
object-group network CSM_INLINE_dst_rule_68719541431
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
!
object-group network PAME-DC-1
 host 192.168.44.111
!
object-group network MSP-DC-1
 description Data Center VSOM
 host 192.168.44.121
!
object-group network CSM_INLINE_dst_rule_68719541435
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object PAME-DC-1
 group-object MSP-DC-1
!
object-group network CSM_INLINE_dst_rule_68719541457
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
!
object-group network CSM_INLINE_dst_rule_68719541461
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
!
object-group network CSM_INLINE_dst_rule_68719541465
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
!
object-group network EMC-NCM
 description EMC Network Configuration Manager
 host 192.168.42.122
!
object-group network RSA-enVision
 description RSA EnVision Syslog collector and SIM
 host 192.168.42.124
!
object-group network CSM_INLINE_dst_rule_73014451187
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object EMC-NCM
 group-object RSA-enVision
!
object-group network TACACS
 description Csico Secure ACS server for TACACS and Radius
 host 192.168.42.131
```

```
!
object-group network RSA-AM
 description RSA Authentication Manager for SecureID
 host 192.168.42.137
!
object-group network NAC-1
 description ISE server for NAC
 host 192.168.42.111
!
object-group network CSM_INLINE_dst_rule_73014451193
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object ActiveDirectory.cisco-irn.com
 group-object TACACS
 group-object RSA-AM
 group-object NAC-1
!
object-group network NAC-2
 host 192.168.42.112
!
object-group network CSM_INLINE_dst_rule_73014451223
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object NAC-2
 group-object NAC-1
!
object-group network DC-Admin
 description DC Admin Systems
 host 192.168.41.101
 host 192.168.41.102
!
object-group network CSManager
 description Cisco Security Manager
 host 192.168.42.133
!
object-group network CSM_INLINE_src_rule_68719541409
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-Admin
 group-object EMC-NCM
 group-object CSManager
!
object-group network CSM_INLINE_src_rule_68719541427
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
!
object-group network CSM_INLINE_src_rule_68719541429
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
!
object-group network CSM_INLINE_src_rule_68719541433
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object PAME-DC-1
 group-object MSP-DC-1
!
object-group network DC-WAAS
 description WAE Appliances in Data Center
 host 192.168.48.10
 host 192.168.49.10
 host 192.168.47.11
 host 192.168.47.12
!
object-group network CSM_INLINE_src_rule_68719541437
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
```

```
 group-object DC-Admin
 group-object DC-WAAS
!
object-group network DC-POS-Tomax
 description Tomax POS Communication from Store to Data Center
 192.168.52.96 255.255.255.224
!
object-group network DC-POS-SAP
 description SAP POS Communication from Store to Data Center
 192.168.52.144 255.255.255.240
!
object-group network DC-POS-Oracle
 description Oracle POS Communication from Store to Data Center
 192.168.52.128 255.255.255.240
!
object-group network CSM_INLINE_src_rule_73014451215
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-Admin
 group-object DC-POS-Tomax
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
!
object-group network CSM_INLINE_src_rule_73014451217
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-Admin
 group-object DC-POS-Tomax
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
!
object-group service CSM_INLINE_svc_rule_68719541409
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq 22
!
object-group service CSM_INLINE_svc_rule_68719541425
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
!
object-group service CSM_INLINE_svc_rule_68719541427
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
!
object-group service LWAPP
 description LWAPP UDP ports 12222 and 12223
 udp eq 12222
 udp eq 12223
!
object-group service TFTP
 description Trivial File Transfer
 tcp eq 69
 udp eq tftp
!
object-group service IP-Protocol-97
 description IP protocol 97
 97
```

```
!
object-group service CSM_INLINE_svc_rule_68719541429
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq www
 tcp eq 22
 tcp eq telnet
 udp eq isakmp
 group-object CAPWAP
 group-object LWAPP
 group-object TFTP
 group-object IP-Protocol-97
!
object-group service Cisco-Mobility
 description Mobility ports for Wireless
 udp eq 16666
 udp eq 16667
!
object-group service CSM_INLINE_svc_rule_68719541431
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 udp eq isakmp
 group-object CAPWAP
 group-object LWAPP
 group-object Cisco-Mobility
 group-object IP-Protocol-97
!
object-group service HTTPS-8443
 tcp eq 8443
!
object-group service Microsoft-DS-SMB
 description Microsoft-DS Active Directory, Windows shares Microsoft-DS SMB file sharing
 tcp eq 445
!
object-group service CSM_INLINE_svc_rule_68719541437
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp
 tcp eq 139
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_68719541439
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp
 tcp eq 139
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_68719541455
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 icmp
 tcp-udp eq 5060
 tcp eq 2000
 tcp eq www
 tcp eq 443
 group-object TFTP
!
object-group service CSM_INLINE_svc_rule_68719541457
```

```
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp-udp eq 5060
 tcp eq 2000
!
object-group service Netbios
 description Netbios Servers
 udp eq netbios-dgm
 udp eq netbios-ns
 tcp eq 139
!
object-group service ORACLE-SIM
 description Oracle Store Inventory Management
 tcp eq 7777
 tcp eq 6003
 tcp range 12401 12500
!
object-group service RDP
 description Windows Remote Desktop
 tcp eq 3389
!
object-group service Workbrain
 tcp eq 8444
!
object-group service CSM_INLINE_svc_rule_68719541459
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq ftp
 tcp eq www
 tcp eq 443
 udp eq 88
 tcp-udp eq 42
 group-object Microsoft-DS-SMB
 group-object Netbios
 group-object ORACLE-SIM
 group-object RDP
 group-object Workbrain
!
object-group service CSM_INLINE_svc_rule_73014451187
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 udp eq syslog
 udp eq snmp
 udp eq snmptrap
!
object-group service CSM_INLINE_svc_rule_73014451193
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq tacacs
 udp eq 1812
 udp eq 1813
 tcp eq 389
 tcp eq 636
!
object-group service vCenter-to-ESX4
 description Communication from vCetner to ESX hosts
 tcp eq 5989
 tcp eq 8000
 tcp eq 902
 tcp eq 903
!
object-group service CSM_INLINE_svc_rule_73014451195
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
```

```
 tcp eq www
 tcp eq 443
 tcp eq 22
 group-object vCenter-to-ESX4
!
object-group service ESX-SLP
 description CIM Service Location Protocol (SLP) for VMware systems
 udp eq 427
 tcp eq 427
!
object-group service CSM_INLINE_svc_rule_73014451197
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 group-object vCenter-to-ESX4
 group-object ESX-SLP
!
object-group service ORACLE-RMI
 description RMI TCP ports 1300 and 1301-1319.
 tcp range 1300 1319
!
object-group service ORACLE-Weblogic
 description HTTP/RMI and HTTPS/RMI-SSL 7001 & 7002. OracleAQ uses 1521.
 tcp eq 7001
 tcp eq 7002
 tcp eq 1521
!
object-group service ORACLE-WAS
 description RMI/IIOP over 2809  HTTP over 9443 IBM-MQ 1414
 tcp eq 2809
 tcp eq 9443
 tcp eq 1414
!
object-group service ORACLE-OAS
 description OAS uses one port for HTTP and RMI - 12601.
 tcp eq 12601
!
object-group service CSM_INLINE_svc_rule_73014451203
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq 22
 group-object ORACLE-RMI
 group-object ORACLE-Weblogic
 group-object ORACLE-WAS
 group-object ORACLE-OAS
!
object-group service CSM_INLINE_svc_rule_73014451205
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq 22
 group-object ORACLE-RMI
 group-object ORACLE-Weblogic
 group-object ORACLE-WAS
 group-object ORACLE-OAS
!
object-group service CSM_INLINE_svc_rule_73014451207
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq 22
 group-object HTTPS-8443
!
```

```
object-group service CSM_INLINE_svc_rule_73014451209
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq 22
 group-object HTTPS-8443
!
object-group service TOMAX-8990
 description Tomax Application Port
 tcp eq 8990
!
object-group service CSM_INLINE_svc_rule_73014451211
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 group-object TOMAX-8990
!
object-group service CSM_INLINE_svc_rule_73014451213
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 group-object TOMAX-8990
!
object-group service ICMP-Requests
 description ICMP requests
 icmp information-request
 icmp mask-request
 icmp timestamp-request
!
object-group service CSM_INLINE_svc_rule_73014451215
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
 icmp redirect
 icmp alternate-address
 group-object ICMP-Requests
!
object-group service CSM_INLINE_svc_rule_73014451217
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
 icmp redirect
 icmp alternate-address
 group-object ICMP-Requests
!
object-group service DNS-Resolving
 description Domain Name Server
 tcp eq domain
 udp eq domain
!
object-group service CSM_INLINE_svc_rule_73014451221
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 udp eq bootps
 group-object DNS-Resolving
!
object-group service CSM_INLINE_svc_rule_73014451223
```

```
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
 group-object HTTPS-8443
!
object-group service CSM_INLINE_svc_rule_73014451388
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp
 tcp eq 139
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_73014451393
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq smtp
 tcp eq pop3
 tcp eq 143
!
object-group service CSM_INLINE_svc_rule_73014451395
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_73014451397
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp
 udp
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_73014451404
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_73014451406
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq smtp
 tcp eq pop3
 tcp eq 143
!
object-group network DC-Applications
 description Applications in the Data Center
 192.168.180.0 255.255.254.0
!
object-group network DC-Voice
 description Data Center Voice
 192.168.45.0 255.255.255.0
!
object-group network MS-Update
 description Windows Update Server
 host 192.168.42.150
!
object-group network MSExchange
 description Mail Server
```

```
 host 192.168.42.140
!
object-group service NTP
 description NTP Protocols
 tcp eq 123
 udp eq ntp
!
object-group network NTP-Servers
 description NTP Servers
 host 192.168.62.161
 host 162.168.62.162
!
object-group network BRANCH-POS
 10.10.0.0 255.255.0.0
!
object-group network vSphere-1
 description vSphere server for Lab
 host 192.168.41.102
!

username bart privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
!
redundancy
!
!
!
!
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh version 2
ip scp server enable
!
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_7
 match protocol http
 match protocol https
 match protocol microsoft-ds
 match protocol ms-sql
 match protocol ms-sql-m
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol oracle
 match protocol oracle-em-vp
 match protocol oraclenames
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_10
 match access-group name CSM_ZBF_CMAP_ACL_10
 match class-map CSM_ZBF_CMAP_PLMAP_7
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_16
 match protocol http
 match protocol https
 match protocol isakmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_23
 match access-group name CSM_ZBF_CMAP_ACL_23
 match class-map CSM_ZBF_CMAP_PLMAP_16
class-map type inspect match-all CSM_ZBF_CLASS_MAP_32
 match access-group name CSM_ZBF_CMAP_ACL_32
class-map type inspect match-all CSM_ZBF_CLASS_MAP_11
 match access-group name CSM_ZBF_CMAP_ACL_11
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_5
```

```
 match protocol http
 match protocol https
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_22
 match access-group name CSM_ZBF_CMAP_ACL_22
 match class-map CSM_ZBF_CMAP_PLMAP_5
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_4
 match protocol http
 match protocol https
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_33
 match access-group name CSM_ZBF_CMAP_ACL_33
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_8
 match protocol sip
 match protocol sip-tls
 match protocol skinny
 match protocol tftp
 match protocol http
 match protocol https
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_12
 match access-group name CSM_ZBF_CMAP_ACL_12
 match class-map CSM_ZBF_CMAP_PLMAP_8
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_15
 match protocol http
 match protocol https
 match protocol netbios-ns
 match protocol netbios-dgm
 match protocol netbios-ssn
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_21
 match access-group name CSM_ZBF_CMAP_ACL_21
 match class-map CSM_ZBF_CMAP_PLMAP_15
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_17
 match protocol http
 match protocol https
 match protocol imap3
 match protocol pop3
 match protocol pop3s
 match protocol smtp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_30
 match access-group name CSM_ZBF_CMAP_ACL_30
 match class-map CSM_ZBF_CMAP_PLMAP_17
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_9
 match protocol syslog
 match protocol syslog-conn
 match protocol snmp
 match protocol snmptrap
class-map type inspect match-all CSM_ZBF_CLASS_MAP_13
 match access-group name CSM_ZBF_CMAP_ACL_13
 match class-map CSM_ZBF_CMAP_PLMAP_9
class-map type inspect match-all CSM_ZBF_CLASS_MAP_20
 match access-group name CSM_ZBF_CMAP_ACL_20
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_20
```

```
 match protocol http
 match protocol https
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
 match protocol ftp
 match protocol ssh
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_31
 match access-group name CSM_ZBF_CMAP_ACL_31
 match class-map CSM_ZBF_CMAP_PLMAP_20
class-map match-all BRANCH-BULK-DATA
 match protocol tftp
 match protocol nfs
 match access-group name BULK-DATA-APPS
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_10
 match protocol ldaps
 match protocol ldap
 match protocol ldap-admin
 match protocol radius
 match protocol tacacs
 match protocol tacacs-ds
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_14
 match access-group name CSM_ZBF_CMAP_ACL_14
 match class-map CSM_ZBF_CMAP_PLMAP_10
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_18
 match protocol http
 match protocol https
 match protocol udp
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_27
 match access-group name CSM_ZBF_CMAP_ACL_27
 match class-map CSM_ZBF_CMAP_PLMAP_18
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_22
 match protocol sip
 match protocol sip-tls
 match protocol skinny
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_36
 match access-group name CSM_ZBF_CMAP_ACL_36
 match class-map CSM_ZBF_CMAP_PLMAP_22
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_11
 match protocol ntp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_15
 match access-group name CSM_ZBF_CMAP_ACL_15
 match class-map CSM_ZBF_CMAP_PLMAP_11
class-map type inspect match-all CSM_ZBF_CLASS_MAP_26
 match access-group name CSM_ZBF_CMAP_ACL_26
 match class-map CSM_ZBF_CMAP_PLMAP_17
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_12
 match protocol bootpc
 match protocol bootps
 match protocol udp
 match protocol tcp
 match protocol dns
 match protocol dhcp-failover
class-map type inspect match-all CSM_ZBF_CLASS_MAP_16
 match access-group name CSM_ZBF_CMAP_ACL_16
 match class-map CSM_ZBF_CMAP_PLMAP_12
```

```
class-map type inspect match-all CSM_ZBF_CLASS_MAP_25
 match access-group name CSM_ZBF_CMAP_ACL_25
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_34
 match access-group name CSM_ZBF_CMAP_ACL_34
class-map type inspect match-all CSM_ZBF_CLASS_MAP_17
 match access-group name CSM_ZBF_CMAP_ACL_17
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_24
 match access-group name CSM_ZBF_CMAP_ACL_24
 match class-map CSM_ZBF_CMAP_PLMAP_7
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_21
 match protocol tcp
 match protocol udp
 match protocol http
 match protocol https
class-map type inspect match-all CSM_ZBF_CLASS_MAP_35
 match access-group name CSM_ZBF_CMAP_ACL_35
 match class-map CSM_ZBF_CMAP_PLMAP_21
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_13
 match protocol https
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_18
 match access-group name CSM_ZBF_CMAP_ACL_18
 match class-map CSM_ZBF_CMAP_PLMAP_13
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_14
 match protocol http
 match protocol https
 match protocol user-8443
class-map type inspect match-all CSM_ZBF_CLASS_MAP_19
 match access-group name CSM_ZBF_CMAP_ACL_19
 match class-map CSM_ZBF_CMAP_PLMAP_14
class-map type inspect match-all CSM_ZBF_CLASS_MAP_29
 match access-group name CSM_ZBF_CMAP_ACL_29
 match class-map CSM_ZBF_CMAP_PLMAP_18
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_19
 match protocol http
 match protocol https
 match protocol icmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_28
 match access-group name CSM_ZBF_CMAP_ACL_28
 match class-map CSM_ZBF_CMAP_PLMAP_19
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_1
 match protocol https
 match protocol ssh
class-map type inspect match-all CSM_ZBF_CLASS_MAP_1
 match access-group name CSM_ZBF_CMAP_ACL_1
 match class-map CSM_ZBF_CMAP_PLMAP_1
class-map type inspect match-all CSM_ZBF_CLASS_MAP_3
 match access-group name CSM_ZBF_CMAP_ACL_3
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_2
 match protocol https
 match protocol http
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_2
 match access-group name CSM_ZBF_CMAP_ACL_2
 match class-map CSM_ZBF_CMAP_PLMAP_2
class-map type inspect match-all CSM_ZBF_CLASS_MAP_5
 match access-group name CSM_ZBF_CMAP_ACL_5
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_3
```

```
 match protocol http
 match protocol https
 match protocol ssh
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_4
 match access-group name CSM_ZBF_CMAP_ACL_4
 match class-map CSM_ZBF_CMAP_PLMAP_3
class-map type inspect match-all CSM_ZBF_CLASS_MAP_7
 match access-group name CSM_ZBF_CMAP_ACL_7
 match class-map CSM_ZBF_CMAP_PLMAP_5
class-map type inspect match-all CSM_ZBF_CLASS_MAP_6
 match access-group name CSM_ZBF_CMAP_ACL_6
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_9
 match access-group name CSM_ZBF_CMAP_ACL_9
 match protocol tcp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_6
 match protocol http
 match protocol https
 match protocol ssh
 match protocol telnet
 match protocol tftp
 match protocol isakmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_8
 match access-group name CSM_ZBF_CMAP_ACL_8
 match class-map CSM_ZBF_CMAP_PLMAP_6
class-map match-all BULK-DATA
 match ip dscp af11  af12
class-map match-all INTERACTIVE-VIDEO
 match ip dscp af41  af42
class-map match-any BRANCH-TRANSACTIONAL-DATA
 match protocol citrix
 match protocol ldap
 match protocol telnet
 match protocol sqlnet
 match protocol http url "*SalesReport*"
 match access-group name TRANSACTIONAL-DATA-APPS
class-map match-all BRANCH-MISSION-CRITICAL
 match access-group name MISSION-CRITICAL-SERVERS
class-map match-all VOICE
 match ip dscp ef
class-map match-all MISSION-CRITICAL-DATA
 match ip dscp 25
class-map match-any BRANCH-NET-MGMT
 match protocol snmp
 match protocol syslog
 match protocol dns
 match protocol icmp
 match protocol ssh
 match access-group name NET-MGMT-APPS
class-map match-all ROUTING
 match ip dscp cs6
class-map match-all SCAVENGER
 match ip dscp cs1
class-map match-all NET-MGMT
 match ip dscp cs2
class-map match-any BRANCH-SCAVENGER
 match protocol gnutella
 match protocol fasttrack
 match protocol kazaa2
class-map match-any CALL-SIGNALING
```

```
 match ip dscp cs3
class-map match-all TRANSACTIONAL-DATA
 match ip dscp af21  af22
!
!
policy-map type inspect CSM_ZBF_POLICY_S_Security_S_POS-W
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_Data_S_POS-W
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_Data-W_S_POS
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_WAN_S_Guest
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_WAN_S_Data-W
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_Voice_S_POS
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_Guest_S_POS
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_MGMT_S_POS-W
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_WLC-AP_S_POS
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_LOOPBACK_S_POS-W
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_WAAS_S_POS-W
 class class-default
  drop log
policy-map BRANCH-LAN-EDGE-OUT
 class class-default
policy-map type inspect CSM_ZBF_POLICY_S_WAAS_S_Partners
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_S_WAAS_S_POS
 class class-default
  drop log
policy-map BRANCH-WAN-EDGE
 class VOICE
  priority percent 18
 class INTERACTIVE-VIDEO
  priority percent 15
 class CALL-SIGNALING
  bandwidth percent 5
 class ROUTING
```

```
  bandwidth percent 3
 class NET-MGMT
  bandwidth percent 2
 class MISSION-CRITICAL-DATA
  bandwidth percent 15
  random-detect
 class TRANSACTIONAL-DATA
  bandwidth percent 12
  random-detect dscp-based
 class BULK-DATA
  bandwidth percent 4
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 1
 class class-default
  bandwidth percent 25
  random-detect
policy-map type inspect CSM_ZBF_POLICY_S_WLC-AP_S_POS-W
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_18
 class type inspect CSM_ZBF_CLASS_MAP_28
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_19
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_29
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_30
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_31
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_16
 class type inspect CSM_ZBF_CLASS_MAP_24
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_25
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_26
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_27
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_17
 class type inspect CSM_ZBF_CLASS_MAP_25
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_26
  inspect Inspect-1
```

```
 class type inspect CSM_ZBF_CLASS_MAP_27
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_14
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_15
 class type inspect CSM_ZBF_CLASS_MAP_13
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_23
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_12
 class type inspect CSM_ZBF_CLASS_MAP_13
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_21
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_30
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_34
  drop log
 class type inspect CSM_ZBF_CLASS_MAP_35
  inspect Inspect-1
 class class-default
  drop
```

```
policy-map type inspect CSM_ZBF_POLICY_S_MGMT_S_POS
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_13
 class type inspect CSM_ZBF_CLASS_MAP_13
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_21
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_20
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_32
  drop log
 class type inspect CSM_ZBF_CLASS_MAP_33
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_10
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_11
 class type inspect CSM_ZBF_CLASS_MAP_13
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_22
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_36
  inspect Inspect-1
 class class-default
  drop log
```

```
policy-map type inspect CSM_ZBF_POLICY_S_Voice_S_POS-W
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_Guest_S_POS-W
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_9
 class type inspect CSM_ZBF_CLASS_MAP_13
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_8
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_12
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_7
 class type inspect CSM_ZBF_CLASS_MAP_9
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_10
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_11
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_6
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_5
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_8
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_4
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_7
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_3
 class type inspect CSM_ZBF_CLASS_MAP_1
```

```
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_5
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_2
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_4
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_1
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_2
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_S_Partners_S_POS
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_Security_S_POS
 class class-default
  drop log
policy-map BRANCH-LAN-EDGE-IN
 class BRANCH-MISSION-CRITICAL
  set ip dscp 25
 class BRANCH-TRANSACTIONAL-DATA
  set ip dscp af21
 class BRANCH-NET-MGMT
  set ip dscp cs2
 class BRANCH-BULK-DATA
  set ip dscp af11
 class BRANCH-SCAVENGER
  set ip dscp cs1
policy-map type inspect CSM_ZBF_POLICY_S_Data_S_POS
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_Data-W_S_POS-W
 class class-default
  drop log
!
zone security S_WAN
 description Store WAN Link
zone security LOOPBACK
 description Loopback interface
zone security S_MGMT
 description VLAN1000 Management
zone security S_Security
 description VLAN20 Physical Security Systems
zone security S_WAAS
 description VLAN19 WAAS optimization
zone security S_WLC-AP
 description VLAN18 Wireless Systems
zone security S_Data
 description VLAN12 Store Data
zone security S_Data-W
```

```
 description VLAN14 Store Wireless Data
zone security S_Guest
 description VLAN17 Guest/Public Wireless
zone security S_Voice
 description VLAN13 Store Voice
zone security S_Partners
 description VLAN16 Partner network
zone security S_POS
 description VLAN 11 POS Data
zone security S_POS-W
 description VLAN15 Store Wireless POS
zone security S_HIPAA
 description VLAN21 HIPAA
zone security S_HIPAA-WU
 description VLAN15 Wireless HIPAA Users
zone security S_HIPAA-WD
 description VLAN15 Wireless HIPAA Devices
zone-pair security CSM_S_WAN-LOOPBACK_1 source S_WAN destination LOOPBACK
 service-policy type inspect CSM_ZBF_POLICY_MAP_1
zone-pair security CSM_S_WAN-S_MGMT_1 source S_WAN destination S_MGMT
 service-policy type inspect CSM_ZBF_POLICY_MAP_2
zone-pair security CSM_S_WAN-S_Security_1 source S_WAN destination S_Security
 service-policy type inspect CSM_ZBF_POLICY_MAP_3
zone-pair security CSM_S_WAN-S_WAAS_1 source S_WAN destination S_WAAS
 service-policy type inspect CSM_ZBF_POLICY_MAP_4
zone-pair security CSM_S_WAN-S_WLC-AP_1 source S_WAN destination S_WLC-AP
 service-policy type inspect CSM_ZBF_POLICY_MAP_5
zone-pair security CSM_S_WAN-S_Data_1 source S_WAN destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Data-W_1 source S_WAN destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_S_WAN_S_Data-W
zone-pair security CSM_S_WAN-S_Guest_1 source S_WAN destination S_Guest
 service-policy type inspect CSM_ZBF_POLICY_S_WAN_S_Guest
zone-pair security CSM_S_WAN-S_Partners_1 source S_WAN destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_POS_1 source S_WAN destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_POS-W_1 source S_WAN destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_HIPAA_1 source S_WAN destination S_HIPAA
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_HIPAA-WU_1 source S_WAN destination S_HIPAA-WU
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_Voice_1 source S_WAN destination S_Voice
 service-policy type inspect CSM_ZBF_POLICY_MAP_8
zone-pair security CSM_LOOPBACK-S_WAN_1 source LOOPBACK destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_9
zone-pair security CSM_LOOPBACK-S_POS_1 source LOOPBACK destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_LOOPBACK-S_POS-W_1 source LOOPBACK destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_LOOPBACK_S_POS-W
zone-pair security CSM_S_MGMT-S_WAN_1 source S_MGMT destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_11
zone-pair security CSM_S_MGMT-S_POS_1 source S_MGMT destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_MGMT_S_POS
zone-pair security CSM_S_MGMT-S_POS-W_1 source S_MGMT destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_S_MGMT_S_POS-W
zone-pair security CSM_S_Security-S_WAN_1 source S_Security destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_12
zone-pair security CSM_S_Security-S_POS_1 source S_Security destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_Security_S_POS
zone-pair security CSM_S_Security-S_POS-W_1 source S_Security destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_S_Security_S_POS-W
zone-pair security CSM_S_WAAS-S_WAN_1 source S_WAAS destination S_WAN
```

```
 service-policy type inspect CSM_ZBF_POLICY_MAP_13
zone-pair security CSM_S_WAAS-S_POS_1 source S_WAAS destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_WAAS_S_POS
zone-pair security CSM_S_WAAS-S_POS-W_1 source S_WAAS destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_S_WAAS_S_POS-W
zone-pair security CSM_S_WAAS-S_Data_1 source S_WAAS destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_Data-W_1 source S_WAAS destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_Partners_1 source S_WAAS destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_S_WAAS_S_Partners
zone-pair security CSM_S_WLC-AP-S_WAN_1 source S_WLC-AP destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_15
zone-pair security CSM_S_WLC-AP-S_POS_1 source S_WLC-AP destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_WLC-AP_S_POS
zone-pair security CSM_S_WLC-AP-S_POS-W_1 source S_WLC-AP destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_S_WLC-AP_S_POS-W
zone-pair security CSM_S_POS-S_WAN_1 source S_POS destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_16
zone-pair security CSM_S_POS-W-S_WAN_1 source S_POS-W destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_17
zone-pair security CSM_S_POS-W-S_POS_1 source S_POS-W destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
zone-pair security CSM_S_Data-S_POS_1 source S_Data destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_Data_S_POS
zone-pair security CSM_S_Data-S_POS-W_1 source S_Data destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_S_Data_S_POS-W
zone-pair security CSM_S_Data-S_WAN_1 source S_Data destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_19
zone-pair security CSM_S_Data-W-S_POS_1 source S_Data-W destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_Data-W_S_POS
zone-pair security CSM_S_Data-W-S_POS-W_1 source S_Data-W destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_S_Data-W_S_POS-W
zone-pair security CSM_S_Data-W-S_WAN_1 source S_Data-W destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_19
zone-pair security CSM_S_Guest-S_POS_1 source S_Guest destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_Guest_S_POS
zone-pair security CSM_S_Guest-S_POS-W_1 source S_Guest destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_S_Guest_S_POS-W
zone-pair security CSM_S_Guest-S_WAN_1 source S_Guest destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_20
zone-pair security CSM_S_Partners-S_POS_1 source S_Partners destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_Partners_S_POS
zone-pair security CSM_S_Partners-S_POS-W_1 source S_Partners destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_Partners-S_WAN_1 source S_Partners destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_21
zone-pair security CSM_S_Voice-S_POS_1 source S_Voice destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_Voice_S_POS
zone-pair security CSM_S_Voice-S_POS-W_1 source S_Voice destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_S_Voice_S_POS-W
zone-pair security CSM_S_Voice-S_WAN_1 source S_Voice destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_22
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.10.158.1 255.255.255.255
 ip pim sparse-dense-mode
 zone-member security LOOPBACK
```

```
!
interface GigabitEthernet0/0
 ip address 10.10.255.144 255.255.255.0
 ip ips Store-IPS in
 ip ips Store-IPS out
 zone-member security S_WAN
 duplex auto
 speed auto
 service-policy output BRANCH-WAN-EDGE
!
interface wlan-ap0
 description Service module interface to manage the embedded AP
 ip address 10.10.158.33 255.255.255.252
 zone-member security S_WLC-AP
 service-module ip address 10.10.158.34 255.255.255.252
 service-module ip default-gateway 10.10.158.33
 arp timeout 0
 no mop enabled
 no mop sysid
!
interface GigabitEthernet0/1
 description ROUTER LINK TO SWITCH
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/1.11
 description POS
 encapsulation dot1Q 11
 ip address 10.10.144.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 ip ips Store-IPS in
 ip ips Store-IPS out
 zone-member security S_POS
 standby 11 ip 10.10.144.1
 standby 11 priority 101
 standby 11 preempt
 ip igmp query-interval 125
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.12
 description DATA
 encapsulation dot1Q 12
 ip address 10.10.145.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip wccp 61 redirect in
 ip pim sparse-dense-mode
 zone-member security S_Data
 standby 12 ip 10.10.145.1
 standby 12 priority 101
 standby 12 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.13
 description VOICE
 encapsulation dot1Q 13
 ip address 10.10.146.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_Voice
 standby 13 ip 10.10.146.1
```

```
 standby 13 priority 101
 standby 13 preempt
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.14
 description WIRELESS
 encapsulation dot1Q 14
 ip address 10.10.147.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Data-W
 standby 14 ip 10.10.147.1
 standby 14 priority 101
 standby 14 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.15
 description WIRELESS-POS
 encapsulation dot1Q 15
 ip address 10.10.148.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip ips Store-IPS in
 ip ips Store-IPS out
 zone-member security S_POS-W
 standby 15 ip 10.10.148.1
 standby 15 priority 101
 standby 15 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.16
 description PARTNER
 encapsulation dot1Q 16
 ip address 10.10.149.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Partners
 standby 16 ip 10.10.149.1
 standby 16 priority 101
 standby 16 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.17
 description WIRELESS-GUEST
 encapsulation dot1Q 17
 ip address 10.10.150.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Guest
 standby 17 ip 10.10.150.1
 standby 17 priority 101
 standby 17 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.18
 description WIRELESS-CONTROL
 encapsulation dot1Q 18
 ip address 10.10.151.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_WLC-AP
 standby 18 ip 10.10.151.1
 standby 18 priority 101
 standby 18 preempt
 service-policy input BRANCH-LAN-EDGE-IN
```

```
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.19
 description WAAS
 encapsulation dot1Q 19
 ip address 10.10.152.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_WAAS
 standby 19 ip 10.10.152.1
 standby 19 priority 101
 standby 19 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.20
 zone-member security S_Security
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.21
 description HIPAA
 encapsulation dot1Q 21
 ip address 10.10.154.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_HIPAA
 standby 21 ip 10.10.154.1
 standby 21 priority 101
 standby 21 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.22
 description WIRELESS-HIPAA-USERS
 encapsulation dot1Q 22
 ip address 10.10.155.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_HIPAA-WU
 standby 22 ip 10.10.155.1
 standby 22 priority 101
 standby 22 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.23
 description WIRELESS-HIPAA-DEVICES
 encapsulation dot1Q 23
 ip address 10.10.156.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_HIPAA-WD
 standby 23 ip 10.10.156.1
 standby 23 priority 101
 standby 23 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet0/1.1000
 description MANAGEMENT
 encapsulation dot1Q 1000
 ip address 10.10.159.2 255.255.255.0
 zone-member security S_MGMT
 standby 100 ip 10.10.159.1
 standby 100 priority 101
```

```
 standby 100 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface Wlan-GigabitEthernet0/0
 description Internal switch interface connecting to the embedded AP
 zone-member security S_WLC-AP
 service-module ip address 10.10.158.34 255.255.255.252
 service-module ip default-gateway 10.10.158.33
!
interface Vlan1
 no ip address
 ip ips Store-IPS in
 ip ips Store-IPS out
 zone-member security S_POS
!
interface Vlan15
 no ip address
 zone-member security S_POS-W
!
interface Vlan1000
 no ip address
 zone-member security S_MGMT
!
router ospf 5
 router-id 10.10.158.1
 passive-interface default
!
no ip forward-protocol nd
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication CiscoACS
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip route 0.0.0.0 0.0.0.0 10.10.255.11
ip tacacs source-interface Loopback0
!
ip access-list extended BULK-DATA-APPS
 remark ---File Transfer---
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
 remark ---E-mail traffic---
 permit tcp any any eq smtp
 permit tcp any any eq pop3
 permit tcp any any eq 143
 remark ---other EDM app protocols---
 permit tcp any any range 3460 3466
 permit tcp any range 3460 3466 any
 remark ---messaging services---
 permit tcp any any eq 2980
 permit tcp any eq 2980 any
 remark ---Microsoft file services---
 permit tcp any any range 137 139
 permit tcp any range 137 139 any
ip access-list extended CSM_ZBF_CMAP_ACL_1
 remark Data Center Mgmt to Devices
 permit object-group CSM_INLINE_svc_rule_68719541409 object-group
CSM_INLINE_src_rule_68719541409 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_10
 remark Permit POS systems to talk to Data Center Servers
```

```
 permit object-group CSM_INLINE_svc_rule_73014451205 object-group DC-POS-Oracle
object-group BRANCH-POS
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451209 object-group DC-POS-SAP object-group
BRANCH-POS
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451213 object-group DC-POS-Tomax
object-group BRANCH-POS
ip access-list extended CSM_ZBF_CMAP_ACL_11
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451215 object-group
CSM_INLINE_src_rule_73014451215 object-group BRANCH-POS
ip access-list extended CSM_ZBF_CMAP_ACL_12
 remark Data Center VOICE (wired and Wireless)
 permit object-group CSM_INLINE_svc_rule_68719541455 object-group DC-Voice object-group
Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_13
 remark Syslog and SNMP Alerts
 permit object-group CSM_INLINE_svc_rule_73014451187 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_73014451187
ip access-list extended CSM_ZBF_CMAP_ACL_14
 remark Store to Data Center Authentications
 permit object-group CSM_INLINE_svc_rule_73014451193 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_73014451193
ip access-list extended CSM_ZBF_CMAP_ACL_15
 remark Store to Data Center for NTP
 permit object-group NTP object-group Branches-ALL object-group NTP-Servers
ip access-list extended CSM_ZBF_CMAP_ACL_16
 remark Store to Data Center for DHCP and DNS
 permit object-group CSM_INLINE_svc_rule_73014451221 object-group Branches-ALL
object-group ActiveDirectory.cisco-irn.com
ip access-list extended CSM_ZBF_CMAP_ACL_17
 remark Permit ICMP traffic
 permit object-group CSM_INLINE_svc_rule_68719541425 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_68719541425
ip access-list extended CSM_ZBF_CMAP_ACL_18
 remark Store UCS E-series server to Data Center vShphere
 permit object-group CSM_INLINE_svc_rule_73014451197 object-group Branches-ALL
object-group vSphere-1
ip access-list extended CSM_ZBF_CMAP_ACL_19
 remark Store NAC
 permit object-group CSM_INLINE_svc_rule_73014451223 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_73014451223
ip access-list extended CSM_ZBF_CMAP_ACL_2
 remark Data Center subscribe to IPS SDEE events
 permit tcp object-group RSA-enVision object-group Branches-ALL eq 443
ip access-list extended CSM_ZBF_CMAP_ACL_20
 remark Store to Data Center Physical Security
 permit ip object-group Branches-ALL object-group CSM_INLINE_dst_rule_68719541435
ip access-list extended CSM_ZBF_CMAP_ACL_21
 remark Store WAAS (WAAS Devices need their own zone)
 permit object-group CSM_INLINE_svc_rule_68719541439 object-group Branches-ALL
object-group DC-WAAS
ip access-list extended CSM_ZBF_CMAP_ACL_22
 remark Store WAAS to Clients and Servers
 permit object-group CSM_INLINE_svc_rule_73014451388 object-group Branches-ALL
object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_23
 remark Store to Data Center wireless controller traffic
 permit object-group CSM_INLINE_svc_rule_68719541431 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_68719541431
ip access-list extended CSM_ZBF_CMAP_ACL_24
 remark Permit POS systems to talk to Data Center Servers
```

```
 permit object-group CSM_INLINE_svc_rule_73014451203 object-group BRANCH-POS object-group
DC-POS-Oracle
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451207 object-group BRANCH-POS object-group
DC-POS-SAP
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451211 object-group BRANCH-POS object-group
DC-POS-Tomax
ip access-list extended CSM_ZBF_CMAP_ACL_25
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451217 object-group
CSM_INLINE_src_rule_73014451217 object-group BRANCH-POS
ip access-list extended CSM_ZBF_CMAP_ACL_26
 remark Store to Data Center for E-mail
 permit object-group CSM_INLINE_svc_rule_73014451393 object-group BRANCH-POS object-group
MSExchange
ip access-list extended CSM_ZBF_CMAP_ACL_27
 remark Store to Data Center for Windows Updates
 permit object-group CSM_INLINE_svc_rule_73014451395 object-group BRANCH-POS object-group
MS-Update
ip access-list extended CSM_ZBF_CMAP_ACL_28
 remark Permit POS clients to talk to branch POS server
 permit object-group CSM_INLINE_svc_rule_73014451397 object-group BRANCH-POS object-group
BRANCH-POS
ip access-list extended CSM_ZBF_CMAP_ACL_29
 remark Store to Data Center for Windows Updates
 permit object-group CSM_INLINE_svc_rule_73014451404 object-group Branches-ALL
object-group MS-Update
ip access-list extended CSM_ZBF_CMAP_ACL_3
 remark Permit ICMP traffic
 permit object-group CSM_INLINE_svc_rule_68719541427 object-group
CSM_INLINE_src_rule_68719541427 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_30
 remark Store to Data Center for E-mail
 permit object-group CSM_INLINE_svc_rule_73014451406 object-group Branches-ALL
object-group MSExchange
ip access-list extended CSM_ZBF_CMAP_ACL_31
 remark Store DATA (wired and Wireless - Access to DC Other applications)
 permit object-group CSM_INLINE_svc_rule_68719541459 object-group Branches-ALL
object-group DC-Applications
ip access-list extended CSM_ZBF_CMAP_ACL_32
 remark Store GUEST - Drop Traffic to Enterprise
 permit ip object-group Branches-ALL object-group CSM_INLINE_dst_rule_68719541465
ip access-list extended CSM_ZBF_CMAP_ACL_33
 remark Store GUEST (access to internet/DMZ web servers)
 permit ip object-group Branches-ALL any
ip access-list extended CSM_ZBF_CMAP_ACL_34
 remark Store PARTNERS - Drop Traffic to Enterprise
 permit ip object-group Branches-ALL object-group CSM_INLINE_dst_rule_68719541461
ip access-list extended CSM_ZBF_CMAP_ACL_35
 remark Store PARTNERS (wired and wireless - Access to Partner site, Internet VPN)
 permit ip object-group Branches-ALL any
ip access-list extended CSM_ZBF_CMAP_ACL_36
 remark Store VOICE (wired and Wireless - Acess to corporate wide voice)
 permit object-group CSM_INLINE_svc_rule_68719541457 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_68719541457
ip access-list extended CSM_ZBF_CMAP_ACL_4
 remark Data Center vSphere to UCS E-series server
 permit object-group CSM_INLINE_svc_rule_73014451195 object-group vSphere-1 object-group
Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_5
 remark Data Center to Store Physical Security
 permit ip object-group CSM_INLINE_src_rule_68719541433 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_6
```

```
 remark Data Center Mgmt to Devices
 permit object-group RDP object-group DC-Admin object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_7
 remark Data Center WAAS to Store
 permit object-group CSM_INLINE_svc_rule_68719541437 object-group
CSM_INLINE_src_rule_68719541437 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_8
 remark Data Center Wireless Control to AP's and Controllers in branchs
 permit object-group CSM_INLINE_svc_rule_68719541429 object-group
CSM_INLINE_src_rule_68719541429 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_9
 remark Data Center Mgmt to Devices
 permit object-group RDP object-group DC-Admin object-group BRANCH-POS
ip access-list extended MISSION-CRITICAL-SERVERS
 remark ---POS Applications---
 permit ip any 192.168.52.0 0.0.0.255
ip access-list extended NET-MGMT-APPS
 remark - Router user Authentication - Identifies TACACS Control traffic
 permit tcp any any eq tacacs
 permit tcp any eq tacacs any
ip access-list extended TRANSACTIONAL-DATA-APPS
 remark ---Workbrain Application---
 remark --Large Store Clock Server to Central Clock Application
 permit tcp host 10.10.49.94 host 192.168.46.72 eq 8444
 remark --Large branch Clock Server to CUAE
 permit tcp host 10.10.49.94 host 192.168.45.185 eq 8000
 remark ---LiteScape Application---
 permit ip any host 192.168.46.82
 permit ip any 239.192.0.0 0.0.0.255
 permit ip any host 239.255.255.250
 remark ---Remote Desktop---
 permit tcp any any eq 3389
 permit tcp any eq 3389 any
 remark ---Oracle SIM---
 permit tcp any 192.168.46.0 0.0.0.255 eq 7777
 permit tcp any 192.168.46.0 0.0.0.255 eq 6003
 permit tcp any 192.168.46.0 0.0.0.255 range 12401 12500
 permit tcp 192.168.46.0 0.0.0.255 eq 7777 any
 permit tcp 192.168.46.0 0.0.0.255 eq 6003 any
 permit tcp 192.168.46.0 0.0.0.255 range 12401 12500 any
!
logging esm config
logging trap debugging
logging source-interface Loopback0
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
!
!
!
!
snmp-server engineID remote 192.168.42.124 0000000000
```

```
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group causer v3 priv
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps flash insertion removal
snmp-server enable traps energywise
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps ipsla
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server domain-stripping
tacacs-server key 7 <removed>
!
!
control-plane
!
!
banner exec C
WARNING:
**** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
**** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner incoming C
WARNING:
**** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
**** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITACCESS IS A
VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner login C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!

!
line con 0
```

```
 session-timeout 15  output
 exec-timeout 15 0
 login authentication CiscoACS
line aux 0
 session-timeout 1  output
 exec-timeout 0 1
 privilege level 0
 login authentication CiscoACS
 no exec
 transport preferred none
 transport output none
line 67
 no activation-character
 no exec
 transport preferred none
 transport output none
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
ntp source Loopback0
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162
end
```

S-A2-MINI-1

```
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname S-A2-Mini-1
!
boot-start-marker
boot-end-marker
!
logging buffered 50000
enable secret 5 <removed>
!
```

```
username bart privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
aaa new-model
!
!
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
system mtu routing 1500
ip subnet-zero
no ip source-route
!
!
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
password encryption aes
!
crypto pki trustpoint TP-self-signed-1919348736
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1919348736
 revocation-check none
 rsakeypair TP-self-signed-1919348736
!
!
crypto pki certificate chain TP-self-signed-1919348736
 certificate self-signed 01
  <removed>
  quit
!
!
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh version 2
ip scp server enable
```

```
!
!
interface GigabitEthernet0/1
 switchport mode trunk
!
interface GigabitEthernet0/2
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/3
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/4
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/5
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/6
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/7
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/8
 switchport mode trunk
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan1000
 description Management VLAN for Switch
 ip address 10.10.159.11 255.255.255.0
 no ip route-cache
!
ip default-gateway 10.10.159.1
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication CiscoACS
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Vlan1000
!
logging trap debugging
logging source-interface Vlan1000
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
```

```
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFF0F
snmp-server trap-source Vlan1000
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps power-ethernet group 1
snmp-server enable traps power-ethernet police
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps energywise
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
!
control-plane
!
banner exec ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                  **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                  **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
```

```
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication CiscoACS
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
!
ntp clock-period 36028654
ntp source Vlan1000
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end
```

S-A2-MINI-2

```
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname S-A2-Mini-2
!
boot-start-marker
boot-end-marker
!
logging buffered 50000
enable secret 5 <removed>
!

username bart privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
```

```
username csmadmin privilege 15 secret 5 <removed>
aaa new-model
!
!
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
system mtu routing 1500
ip subnet-zero
no ip source-route
!
!
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
password encryption aes
!
crypto pki trustpoint TP-self-signed-1919334912
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1919334912
 revocation-check none
 rsakeypair TP-self-signed-1919334912
!
!
crypto pki certificate chain TP-self-signed-1919334912
 certificate self-signed 01
  <removed>
  quit
!
!
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh version 2
ip scp server enable
!
!
interface GigabitEthernet0/1
```

```
 description AIR-CAP3502E
 switchport trunk native vlan 18
 switchport trunk allowed vlan 14-18
 switchport mode trunk
!
interface GigabitEthernet0/2
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/3
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/4
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/5
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/6
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/7
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/8
 switchport mode trunk
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan1000
 description Management VLAN for Switch
 ip address 10.10.159.12 255.255.255.0
 no ip route-cache
!
ip default-gateway 10.10.159.1
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication CiscoACS
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Vlan1000
!
logging trap debugging
logging source-interface Vlan1000
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
```

```
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
snmp-server trap-source Vlan1000
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps power-ethernet group 1
snmp-server enable traps power-ethernet police
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps energywise
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
!
control-plane
!
banner exec ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                  **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                  **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
```

```
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication CiscoACS
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
!
ntp clock-period 36028680
ntp source Vlan1000
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end
```

Doctor's Office

R-A2-CONV-1

```
version 15.1
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
no service password-recovery
!
hostname R-A2-Conv-1
!
boot-start-marker
boot system flash c890-universalk9-mz.151-3.T.bin
boot-end-marker
!
```

```
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 50000
no logging rate-limit
enable secret 5 <removed>
!
aaa new-model
!
!
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default
 action-type start-stop
 group tacacs+
!
aaa accounting commands 15 default
 action-type start-stop
 group tacacs+
!
aaa accounting system default
 action-type start-stop
 group tacacs+
!
!
!
!
!
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PST recurring
service-module wlan-ap 0 bootimage autonomous
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-479252603
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-479252603
 revocation-check none
 rsakeypair TP-self-signed-479252603
!
!
crypto pki certificate chain TP-self-signed-479252603
 certificate self-signed 01
  <removed>
    quit
no ip source-route
!
!
!
!
!
ip cef
no ip bootp server
ip domain name cisco-irn.com
ip name-server 192.168.42.130
ip multicast-routing
ip port-map user-8443 port tcp 8443
ip ips config location flash: retries 1 timeout 1
ip ips name Store-IPS
!
```

```
ip ips signature-category
  category all
   retired true
  category ios_ips default
   retired false
!
ip inspect log drop-pkt
ip inspect audit-trail
ip wccp 61
ip wccp 62
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
no ipv6 cef
!
multilink bundle-name authenticated
parameter-map type inspect Inspect-1
 audit-trail on
parameter-map type inspect global
 WAAS enable

parameter-map type trend-global trend-glob-map
password encryption aes
license udi pid CISCO891W-AGN-N-K9 sn <removed>
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
object-group network ActiveDirectory.cisco-irn.com
 host 192.168.42.130
!
object-group service CAPWAP
 description CAPWAP UDP ports 5246 and 5247
 udp eq 5246
 udp eq 5247
!
object-group service CISCO-WAAS
 description Ports for Cisco WAAS
 tcp eq 4050
!
object-group network DC-ALL
 description All of the Data Center
 192.168.0.0 255.255.0.0
!
object-group network Branches-ALL
 description all branch networks
 10.10.0.0 255.255.0.0
!
object-group network CSM_INLINE_dst_rule_68719541425
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
!
object-group network WCSManager
 description Wireless Manager
 host 192.168.43.135
!
object-group network DC-Wifi-Controllers
 description Central Wireless Controllers for branchs
 host 192.168.43.21
```

```
 host 192.168.43.22
!
object-group network DC-Wifi-MSE
 description Mobility Service Engines
 host 192.168.43.31
 host 192.168.43.32
!
object-group network CSM_INLINE_dst_rule_68719541431
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
!
object-group network PAME-DC-1
 host 192.168.44.111
!
object-group network MSP-DC-1
 description Data Center VSOM
 host 192.168.44.121
!
object-group network CSM_INLINE_dst_rule_68719541435
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object PAME-DC-1
 group-object MSP-DC-1
!
object-group network CSM_INLINE_dst_rule_68719541457
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
!
object-group network CSM_INLINE_dst_rule_68719541461
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
!
object-group network CSM_INLINE_dst_rule_68719541465
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
!
object-group network EMC-NCM
 description EMC Network Configuration Manager
 host 192.168.42.122
!
object-group network RSA-enVision
 description RSA EnVision Syslog collector and SIM
 host 192.168.42.124
!
object-group network CSM_INLINE_dst_rule_73014451187
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object EMC-NCM
 group-object RSA-enVision
!
object-group network TACACS
 description Csico Secure ACS server for TACACS and Radius
 host 192.168.42.131
!
object-group network RSA-AM
 description RSA Authentication Manager for SecureID
 host 192.168.42.137
!
object-group network NAC-1
 description ISE server for NAC
 host 192.168.42.111
```

```
!
object-group network CSM_INLINE_dst_rule_73014451193
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object ActiveDirectory.cisco-irn.com
 group-object TACACS
 group-object RSA-AM
 group-object NAC-1
!
object-group network NAC-2
 host 192.168.42.112
!
object-group network CSM_INLINE_dst_rule_73014451223
 description Generated by CS-Manager from dst of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object NAC-2
 group-object NAC-1
!
object-group network DC-Admin
 description DC Admin Systems
 host 192.168.41.101
 host 192.168.41.102
!
object-group network CSManager
 description Cisco Security Manager
 host 192.168.42.133
!
object-group network CSM_INLINE_src_rule_68719541409
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-Admin
 group-object EMC-NCM
 group-object CSManager
!
object-group network CSM_INLINE_src_rule_68719541427
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-ALL
 group-object Branches-ALL
!
object-group network CSM_INLINE_src_rule_68719541429
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
!
object-group network CSM_INLINE_src_rule_68719541433
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object PAME-DC-1
 group-object MSP-DC-1
!
object-group network DC-WAAS
 description WAE Appliances in Data Center
 host 192.168.48.10
 host 192.168.49.10
 host 192.168.47.11
 host 192.168.47.12
!
object-group network CSM_INLINE_src_rule_68719541437
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-Admin
 group-object DC-WAAS
!
object-group network DC-POS-Tomax
 description Tomax POS Communication from Store to Data Center
 192.168.52.96 255.255.255.224
!
object-group network DC-POS-SAP
```

```
 description SAP POS Communication from Store to Data Center
 192.168.52.144 255.255.255.240
!
object-group network DC-POS-Oracle
 description Oracle POS Communication from Store to Data Center
 192.168.52.128 255.255.255.240
!
object-group network CSM_INLINE_src_rule_73014451215
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-Admin
 group-object DC-POS-Tomax
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
!
object-group network CSM_INLINE_src_rule_73014451217
 description Generated by CS-Manager from src of ZbfInspectRule# 0 (Store-Small/mandatory)
 group-object DC-Admin
 group-object DC-POS-Tomax
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
!
object-group service CSM_INLINE_svc_rule_68719541409
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq 22
!
object-group service CSM_INLINE_svc_rule_68719541425
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
!
object-group service CSM_INLINE_svc_rule_68719541427
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
!
object-group service LWAPP
 description LWAPP UDP ports 12222 and 12223
 udp eq 12222
 udp eq 12223
!
object-group service TFTP
 description Trivial File Transfer
 tcp eq 69
 udp eq tftp
!
object-group service IP-Protocol-97
 description IP protocol 97
 97
!
object-group service CSM_INLINE_svc_rule_68719541429
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq www
 tcp eq 22
 tcp eq telnet
```

```
 udp eq isakmp
 group-object CAPWAP
 group-object LWAPP
 group-object TFTP
 group-object IP-Protocol-97
!
object-group service Cisco-Mobility
 description Mobility ports for Wireless
 udp eq 16666
 udp eq 16667
!
object-group service CSM_INLINE_svc_rule_68719541431
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 udp eq isakmp
 group-object CAPWAP
 group-object LWAPP
 group-object Cisco-Mobility
 group-object IP-Protocol-97
!
object-group service HTTPS-8443
 tcp eq 8443
!
object-group service Microsoft-DS-SMB
 description Microsoft-DS Active Directory, Windows shares Microsoft-DS SMB file sharing
 tcp eq 445
!
object-group service CSM_INLINE_svc_rule_68719541437
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp
 tcp eq 139
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_68719541439
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp
 tcp eq 139
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_68719541455
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 icmp
 tcp-udp eq 5060
 tcp eq 2000
 tcp eq www
 tcp eq 443
 group-object TFTP
!
object-group service CSM_INLINE_svc_rule_68719541457
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp-udp eq 5060
 tcp eq 2000
!
object-group service Netbios
 description Netbios Servers
 udp eq netbios-dgm
```

```
 udp eq netbios-ns
 tcp eq 139
!
object-group service ORACLE-SIM
 description Oracle Store Inventory Management
 tcp eq 7777
 tcp eq 6003
 tcp range 12401 12500
!
object-group service RDP
 description Windows Remote Desktop
 tcp eq 3389
!
object-group service Workbrain
 tcp eq 8444
!
object-group service CSM_INLINE_svc_rule_68719541459
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq ftp
 tcp eq www
 tcp eq 443
 udp eq 88
 tcp-udp eq 42
 group-object Microsoft-DS-SMB
 group-object Netbios
 group-object ORACLE-SIM
 group-object RDP
 group-object Workbrain
!
object-group service CSM_INLINE_svc_rule_73014451187
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 udp eq syslog
 udp eq snmp
 udp eq snmptrap
!
object-group service CSM_INLINE_svc_rule_73014451193
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq tacacs
 udp eq 1812
 udp eq 1813
 tcp eq 389
 tcp eq 636
!
object-group service vCenter-to-ESX4
 description Communication from vCetner to ESX hosts
 tcp eq 5989
 tcp eq 8000
 tcp eq 902
 tcp eq 903
!
object-group service CSM_INLINE_svc_rule_73014451195
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq 22
 group-object vCenter-to-ESX4
!
object-group service ESX-SLP
 description CIM Service Location Protocol (SLP) for VMware systems
 udp eq 427
```

```
 tcp eq 427
!
object-group service CSM_INLINE_svc_rule_73014451197
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 group-object vCenter-to-ESX4
 group-object ESX-SLP
!
object-group service ORACLE-RMI
 description RMI TCP ports 1300 and 1301-1319.
 tcp range 1300 1319
!
object-group service ORACLE-Weblogic
 description HTTP/RMI and HTTPS/RMI-SSL 7001 & 7002. OracleAQ uses 1521.
 tcp eq 7001
 tcp eq 7002
 tcp eq 1521
!
object-group service ORACLE-WAS
 description RMI/IIOP over 2809  HTTP over 9443 IBM-MQ 1414
 tcp eq 2809
 tcp eq 9443
 tcp eq 1414
!
object-group service ORACLE-OAS
 description OAS uses one port for HTTP and RMI - 12601.
 tcp eq 12601
!
object-group service CSM_INLINE_svc_rule_73014451203
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq 22
 group-object ORACLE-RMI
 group-object ORACLE-Weblogic
 group-object ORACLE-WAS
 group-object ORACLE-OAS
!
object-group service CSM_INLINE_svc_rule_73014451205
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq 22
 group-object ORACLE-RMI
 group-object ORACLE-Weblogic
 group-object ORACLE-WAS
 group-object ORACLE-OAS
!
object-group service CSM_INLINE_svc_rule_73014451207
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq 22
 group-object HTTPS-8443
!
object-group service CSM_INLINE_svc_rule_73014451209
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 tcp eq 22
 group-object HTTPS-8443
!
object-group service TOMAX-8990
```

```
 description Tomax Application Port
 tcp eq 8990
!
object-group service CSM_INLINE_svc_rule_73014451211
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 group-object TOMAX-8990
!
object-group service CSM_INLINE_svc_rule_73014451213
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq 443
 group-object TOMAX-8990
!
object-group service ICMP-Requests
 description ICMP requests
 icmp information-request
 icmp mask-request
 icmp timestamp-request
!
object-group service CSM_INLINE_svc_rule_73014451215
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
 icmp redirect
 icmp alternate-address
 group-object ICMP-Requests
!
object-group service CSM_INLINE_svc_rule_73014451217
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 icmp echo
 icmp echo-reply
 icmp traceroute
 icmp unreachable
 icmp redirect
 icmp alternate-address
 group-object ICMP-Requests
!
object-group service DNS-Resolving
 description Domain Name Server
 tcp eq domain
 udp eq domain
!
object-group service CSM_INLINE_svc_rule_73014451221
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 udp eq bootps
 group-object DNS-Resolving
!
object-group service CSM_INLINE_svc_rule_73014451223
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
 group-object HTTPS-8443
!
object-group service CSM_INLINE_svc_rule_73014451388
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
```

```
 tcp
 tcp eq 139
 group-object Microsoft-DS-SMB
!
object-group service CSM_INLINE_svc_rule_73014451393
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq smtp
 tcp eq pop3
 tcp eq 143
!
object-group service CSM_INLINE_svc_rule_73014451395
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_73014451397
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp
 udp
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_73014451404
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
!
object-group service CSM_INLINE_svc_rule_73014451406
 description Generated by CS-Manager from service of ZbfInspectRule# 0
(Store-Small/mandatory)
 tcp eq www
 tcp eq 443
 tcp eq smtp
 tcp eq pop3
 tcp eq 143
!
object-group network DC-Applications
 description Applications in the Data Center
 192.168.180.0 255.255.254.0
!
object-group network DC-Voice
 description Data Center Voice
 192.168.45.0 255.255.255.0
!
object-group network MS-Update
 description Windows Update Server
 host 192.168.42.150
!
object-group network MSExchange
 description Mail Server
 host 192.168.42.140
!
object-group service NTP
 description NTP Protocols
 tcp eq 123
 udp eq ntp
!
object-group network NTP-Servers
 description NTP Servers
```

```
 host 192.168.62.161
 host 162.168.62.162
!
object-group network BRANCH-POS
 10.10.0.0 255.255.0.0
!
object-group network vSphere-1
 description vSphere server for Lab
 host 192.168.41.102
!

username bart privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
!
!
!
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh version 2
ip scp server enable
!
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_7
 match protocol http
 match protocol https
 match protocol microsoft-ds
 match protocol ms-sql
 match protocol ms-sql-m
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol oracle
 match protocol oracle-em-vp
 match protocol oraclenames
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_10
 match access-group name CSM_ZBF_CMAP_ACL_10
 match class-map CSM_ZBF_CMAP_PLMAP_7
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_16
 match protocol http
 match protocol https
 match protocol isakmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_23
 match access-group name CSM_ZBF_CMAP_ACL_23
 match class-map CSM_ZBF_CMAP_PLMAP_16
class-map type inspect match-all CSM_ZBF_CLASS_MAP_32
 match access-group name CSM_ZBF_CMAP_ACL_32
class-map type inspect match-all CSM_ZBF_CLASS_MAP_11
 match access-group name CSM_ZBF_CMAP_ACL_11
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_5
 match protocol http
 match protocol https
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_22
 match access-group name CSM_ZBF_CMAP_ACL_22
 match class-map CSM_ZBF_CMAP_PLMAP_5
```

```
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_4
 match protocol http
 match protocol https
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_33
 match access-group name CSM_ZBF_CMAP_ACL_33
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_8
 match protocol sip
 match protocol sip-tls
 match protocol skinny
 match protocol tftp
 match protocol http
 match protocol https
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_12
 match access-group name CSM_ZBF_CMAP_ACL_12
 match class-map CSM_ZBF_CMAP_PLMAP_8
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_15
 match protocol http
 match protocol https
 match protocol netbios-ns
 match protocol netbios-dgm
 match protocol netbios-ssn
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_21
 match access-group name CSM_ZBF_CMAP_ACL_21
 match class-map CSM_ZBF_CMAP_PLMAP_15
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_17
 match protocol http
 match protocol https
 match protocol imap3
 match protocol pop3
 match protocol pop3s
 match protocol smtp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_30
 match access-group name CSM_ZBF_CMAP_ACL_30
 match class-map CSM_ZBF_CMAP_PLMAP_17
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_9
 match protocol syslog
 match protocol syslog-conn
 match protocol snmp
 match protocol snmptrap
class-map type inspect match-all CSM_ZBF_CLASS_MAP_13
 match access-group name CSM_ZBF_CMAP_ACL_13
 match class-map CSM_ZBF_CMAP_PLMAP_9
class-map type inspect match-all CSM_ZBF_CLASS_MAP_20
 match access-group name CSM_ZBF_CMAP_ACL_20
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_20
 match protocol http
 match protocol https
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
 match protocol ftp
 match protocol ssh
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_31
```

```
 match access-group name CSM_ZBF_CMAP_ACL_31
 match class-map CSM_ZBF_CMAP_PLMAP_20
class-map match-all BRANCH-BULK-DATA
 match protocol tftp
 match protocol nfs
 match access-group name BULK-DATA-APPS
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_10
 match protocol ldaps
 match protocol ldap
 match protocol ldap-admin
 match protocol radius
 match protocol tacacs
 match protocol tacacs-ds
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_14
 match access-group name CSM_ZBF_CMAP_ACL_14
 match class-map CSM_ZBF_CMAP_PLMAP_10
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_18
 match protocol http
 match protocol https
 match protocol udp
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_27
 match access-group name CSM_ZBF_CMAP_ACL_27
 match class-map CSM_ZBF_CMAP_PLMAP_18
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_22
 match protocol sip
 match protocol sip-tls
 match protocol skinny
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_36
 match access-group name CSM_ZBF_CMAP_ACL_36
 match class-map CSM_ZBF_CMAP_PLMAP_22
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_11
 match protocol ntp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_15
 match access-group name CSM_ZBF_CMAP_ACL_15
 match class-map CSM_ZBF_CMAP_PLMAP_11
class-map type inspect match-all CSM_ZBF_CLASS_MAP_26
 match access-group name CSM_ZBF_CMAP_ACL_26
 match class-map CSM_ZBF_CMAP_PLMAP_17
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_12
 match protocol bootpc
 match protocol bootps
 match protocol udp
 match protocol tcp
 match protocol dns
 match protocol dhcp-failover
class-map type inspect match-all CSM_ZBF_CLASS_MAP_16
 match access-group name CSM_ZBF_CMAP_ACL_16
 match class-map CSM_ZBF_CMAP_PLMAP_12
class-map type inspect match-all CSM_ZBF_CLASS_MAP_25
 match access-group name CSM_ZBF_CMAP_ACL_25
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_34
 match access-group name CSM_ZBF_CMAP_ACL_34
class-map type inspect match-all CSM_ZBF_CLASS_MAP_17
 match access-group name CSM_ZBF_CMAP_ACL_17
 match protocol icmp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_24
 match access-group name CSM_ZBF_CMAP_ACL_24
```

```
 match class-map CSM_ZBF_CMAP_PLMAP_7
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_21
 match protocol tcp
 match protocol udp
 match protocol http
 match protocol https
class-map type inspect match-all CSM_ZBF_CLASS_MAP_35
 match access-group name CSM_ZBF_CMAP_ACL_35
 match class-map CSM_ZBF_CMAP_PLMAP_21
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_13
 match protocol https
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_18
 match access-group name CSM_ZBF_CMAP_ACL_18
 match class-map CSM_ZBF_CMAP_PLMAP_13
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_14
 match protocol http
 match protocol https
 match protocol user-8443
class-map type inspect match-all CSM_ZBF_CLASS_MAP_19
 match access-group name CSM_ZBF_CMAP_ACL_19
 match class-map CSM_ZBF_CMAP_PLMAP_14
class-map type inspect match-all CSM_ZBF_CLASS_MAP_29
 match access-group name CSM_ZBF_CMAP_ACL_29
 match class-map CSM_ZBF_CMAP_PLMAP_18
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_19
 match protocol http
 match protocol https
 match protocol icmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_28
 match access-group name CSM_ZBF_CMAP_ACL_28
 match class-map CSM_ZBF_CMAP_PLMAP_19
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_1
 match protocol https
 match protocol ssh
class-map type inspect match-all CSM_ZBF_CLASS_MAP_1
 match access-group name CSM_ZBF_CMAP_ACL_1
 match class-map CSM_ZBF_CMAP_PLMAP_1
class-map type inspect match-all CSM_ZBF_CLASS_MAP_3
 match access-group name CSM_ZBF_CMAP_ACL_3
 match protocol icmp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_2
 match protocol https
 match protocol http
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_2
 match access-group name CSM_ZBF_CMAP_ACL_2
 match class-map CSM_ZBF_CMAP_PLMAP_2
class-map type inspect match-all CSM_ZBF_CLASS_MAP_5
 match access-group name CSM_ZBF_CMAP_ACL_5
 match class-map CSM_ZBF_CMAP_PLMAP_4
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_3
 match protocol http
 match protocol https
 match protocol ssh
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_4
 match access-group name CSM_ZBF_CMAP_ACL_4
 match class-map CSM_ZBF_CMAP_PLMAP_3
class-map type inspect match-all CSM_ZBF_CLASS_MAP_7
 match access-group name CSM_ZBF_CMAP_ACL_7
```

```
 match class-map CSM_ZBF_CMAP_PLMAP_5
class-map type inspect match-all CSM_ZBF_CLASS_MAP_6
 match access-group name CSM_ZBF_CMAP_ACL_6
 match protocol tcp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_9
 match access-group name CSM_ZBF_CMAP_ACL_9
 match protocol tcp
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_6
 match protocol http
 match protocol https
 match protocol ssh
 match protocol telnet
 match protocol tftp
 match protocol isakmp
 match protocol tcp
 match protocol udp
class-map type inspect match-all CSM_ZBF_CLASS_MAP_8
 match access-group name CSM_ZBF_CMAP_ACL_8
 match class-map CSM_ZBF_CMAP_PLMAP_6
class-map match-all BULK-DATA
 match ip dscp af11  af12
class-map match-all INTERACTIVE-VIDEO
 match ip dscp af41  af42
class-map match-any BRANCH-TRANSACTIONAL-DATA
 match protocol citrix
 match protocol ldap
 match protocol telnet
 match protocol sqlnet
 match protocol http url "*SalesReport*"
 match access-group name TRANSACTIONAL-DATA-APPS
class-map match-all BRANCH-MISSION-CRITICAL
 match access-group name MISSION-CRITICAL-SERVERS
class-map match-all VOICE
 match ip dscp ef
class-map match-all MISSION-CRITICAL-DATA
 match ip dscp 25
class-map match-any BRANCH-NET-MGMT
 match protocol snmp
 match protocol syslog
 match protocol dns
 match protocol icmp
 match protocol ssh
 match access-group name NET-MGMT-APPS
class-map match-all ROUTING
 match ip dscp cs6
class-map match-all SCAVENGER
 match ip dscp cs1
class-map match-all NET-MGMT
 match ip dscp cs2
class-map match-any BRANCH-SCAVENGER
 match protocol gnutella
 match protocol fasttrack
 match protocol kazaa2
class-map match-any CALL-SIGNALING
 match ip dscp cs3
class-map match-all TRANSACTIONAL-DATA
 match ip dscp af21  af22
!
!
policy-map type inspect CSM_ZBF_POLICY_S_Security_S_POS-W
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_Data_S_POS-W
 class class-default
```

```
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_Data-W_S_POS
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_WAN_S_Guest
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_WAN_S_Data-W
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_Voice_S_POS
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_Guest_S_POS
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_MGMT_S_POS-W
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_WLC-AP_S_POS
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_LOOPBACK_S_POS-W
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_WAAS_S_POS-W
 class class-default
  drop log
policy-map BRANCH-LAN-EDGE-OUT
 class class-default
policy-map type inspect CSM_ZBF_POLICY_S_WAAS_S_Partners
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_S_WAAS_S_POS
 class class-default
  drop log
policy-map BRANCH-WAN-EDGE
 class VOICE
  priority percent 18
 class INTERACTIVE-VIDEO
  priority percent 15
 class CALL-SIGNALING
  bandwidth percent 5
 class ROUTING
  bandwidth percent 3
 class NET-MGMT
  bandwidth percent 2
 class MISSION-CRITICAL-DATA
  bandwidth percent 15
  random-detect
 class TRANSACTIONAL-DATA
  bandwidth percent 12
  random-detect dscp-based
 class BULK-DATA
```

```
  bandwidth percent 4
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 1
 class class-default
  bandwidth percent 25
  random-detect
policy-map type inspect CSM_ZBF_POLICY_S_WLC-AP_S_POS-W
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_18
 class type inspect CSM_ZBF_CLASS_MAP_28
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_19
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_29
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_30
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_31
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_16
 class type inspect CSM_ZBF_CLASS_MAP_24
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_25
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_26
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_27
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_17
 class type inspect CSM_ZBF_CLASS_MAP_25
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_26
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_27
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class class-default
  drop
```

```
policy-map type inspect CSM_ZBF_POLICY_MAP_14
 class type inspect CSM_ZBF_CLASS_MAP_22
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_15
 class type inspect CSM_ZBF_CLASS_MAP_13
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_23
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_12
 class type inspect CSM_ZBF_CLASS_MAP_13
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_20
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_21
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_30
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_34
  drop log
 class type inspect CSM_ZBF_CLASS_MAP_35
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_S_MGMT_S_POS
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_13
 class type inspect CSM_ZBF_CLASS_MAP_13
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
```

```
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_21
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_20
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_32
  drop log
 class type inspect CSM_ZBF_CLASS_MAP_33
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_10
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_11
 class type inspect CSM_ZBF_CLASS_MAP_13
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_18
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_22
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_19
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_36
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_Voice_S_POS-W
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_Guest_S_POS-W
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_9
 class type inspect CSM_ZBF_CLASS_MAP_13
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_14
```

```
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_15
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_16
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_17
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_MAP_8
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_12
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_7
 class type inspect CSM_ZBF_CLASS_MAP_9
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_10
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_11
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_6
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_5
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_8
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_4
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_6
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_7
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_3
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_5
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_2
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
```

```
 class type inspect CSM_ZBF_CLASS_MAP_4
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_MAP_1
 class type inspect CSM_ZBF_CLASS_MAP_1
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_2
  inspect Inspect-1
 class type inspect CSM_ZBF_CLASS_MAP_3
  inspect Inspect-1
 class class-default
  drop
policy-map type inspect CSM_ZBF_POLICY_S_Partners_S_POS
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_Security_S_POS
 class class-default
  drop log
policy-map BRANCH-LAN-EDGE-IN
 class BRANCH-MISSION-CRITICAL
  set ip dscp 25
 class BRANCH-TRANSACTIONAL-DATA
  set ip dscp af21
 class BRANCH-NET-MGMT
  set ip dscp cs2
 class BRANCH-BULK-DATA
  set ip dscp af11
 class BRANCH-SCAVENGER
  set ip dscp cs1
policy-map type inspect CSM_ZBF_POLICY_S_Data_S_POS
 class class-default
  drop log
policy-map type inspect CSM_ZBF_POLICY_S_Data-W_S_POS-W
 class class-default
  drop log
!
zone security S_WAN
 description Store WAN Link
zone security LOOPBACK
 description Loopback interface
zone security S_MGMT
 description VLAN1000 Management
zone security S_Security
 description VLAN20 Physical Security Systems
zone security S_WAAS
 description VLAN19 WAAS optimization
zone security S_WLC-AP
 description VLAN18 Wireless Systems
zone security S_Data
 description VLAN12 Store Data
zone security S_Data-W
 description VLAN14 Store Wireless Data
zone security S_Guest
 description VLAN17 Guest/Public Wireless
zone security S_Voice
 description VLAN13 Store Voice
zone security S_Partners
 description VLAN16 Partner network
zone security S_POS
 description VLAN 11 POS Data
zone security S_POS-W
```

```
 description VLAN15 Store Wireless POS
zone security S_HIPAA
 description VLAN21 HIPAA
zone security S_HIPAA-WU
 description VLAN15 Wireless HIPAA Users
zone security S_HIPAA-WD
 description VLAN15 Wireless HIPAA Devices
zone-pair security CSM_S_WAN-LOOPBACK_1 source S_WAN destination LOOPBACK
 service-policy type inspect CSM_ZBF_POLICY_MAP_1
zone-pair security CSM_S_WAN-S_MGMT_1 source S_WAN destination S_MGMT
 service-policy type inspect CSM_ZBF_POLICY_MAP_2
zone-pair security CSM_S_WAN-S_Security_1 source S_WAN destination S_Security
 service-policy type inspect CSM_ZBF_POLICY_MAP_3
zone-pair security CSM_S_WAN-S_WAAS_1 source S_WAN destination S_WAAS
 service-policy type inspect CSM_ZBF_POLICY_MAP_4
zone-pair security CSM_S_WAN-S_WLC-AP_1 source S_WAN destination S_WLC-AP
 service-policy type inspect CSM_ZBF_POLICY_MAP_5
zone-pair security CSM_S_WAN-S_Data_1 source S_WAN destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_Data-W_1 source S_WAN destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_S_WAN_S_Data-W
zone-pair security CSM_S_WAN-S_Guest_1 source S_WAN destination S_Guest
 service-policy type inspect CSM_ZBF_POLICY_S_WAN_S_Guest
zone-pair security CSM_S_WAN-S_Partners_1 source S_WAN destination S_Partners
 service-policy type inspect CSM_ZBF_POLICY_MAP_6
zone-pair security CSM_S_WAN-S_POS_1 source S_WAN destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_POS-W_1 source S_WAN destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_HIPAA_1 source S_WAN destination S_HIPAA
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_HIPAA-WU_1 source S_WAN destination S_HIPAA-WU
 service-policy type inspect CSM_ZBF_POLICY_MAP_7
zone-pair security CSM_S_WAN-S_Voice_1 source S_WAN destination S_Voice
 service-policy type inspect CSM_ZBF_POLICY_MAP_8
zone-pair security CSM_LOOPBACK-S_WAN_1 source LOOPBACK destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_9
zone-pair security CSM_LOOPBACK-S_POS_1 source LOOPBACK destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_LOOPBACK-S_POS-W_1 source LOOPBACK destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_LOOPBACK_S_POS-W
zone-pair security CSM_S_MGMT-S_WAN_1 source S_MGMT destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_11
zone-pair security CSM_S_MGMT-S_POS_1 source S_MGMT destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_MGMT_S_POS
zone-pair security CSM_S_MGMT-S_POS-W_1 source S_MGMT destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_S_MGMT_S_POS-W
zone-pair security CSM_S_Security-S_WAN_1 source S_Security destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_12
zone-pair security CSM_S_Security-S_POS_1 source S_Security destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_Security_S_POS
zone-pair security CSM_S_Security-S_POS-W_1 source S_Security destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_S_Security_S_POS-W
zone-pair security CSM_S_WAAS-S_WAN_1 source S_WAAS destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_13
zone-pair security CSM_S_WAAS-S_POS_1 source S_WAAS destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_WAAS_S_POS
zone-pair security CSM_S_WAAS-S_POS-W_1 source S_WAAS destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_S_WAAS_S_POS-W
zone-pair security CSM_S_WAAS-S_Data_1 source S_WAAS destination S_Data
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_Data-W_1 source S_WAAS destination S_Data-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_14
zone-pair security CSM_S_WAAS-S_Partners_1 source S_WAAS destination S_Partners
```

```
 service-policy type inspect CSM_ZBF_POLICY_S_WAAS_S_Partners
zone-pair security CSM_S_WLC-AP-S_WAN_1 source S_WLC-AP destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_15
zone-pair security CSM_S_WLC-AP-S_POS_1 source S_WLC-AP destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_WLC-AP_S_POS
zone-pair security CSM_S_WLC-AP-S_POS-W_1 source S_WLC-AP destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_S_WLC-AP_S_POS-W
zone-pair security CSM_S_POS-S_WAN_1 source S_POS destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_16
zone-pair security CSM_S_POS-W-S_WAN_1 source S_POS-W destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_17
zone-pair security CSM_S_POS-W-S_POS_1 source S_POS-W destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
zone-pair security CSM_S_Data-S_POS_1 source S_Data destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_Data_S_POS
zone-pair security CSM_S_Data-S_POS-W_1 source S_Data destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_S_Data_S_POS-W
zone-pair security CSM_S_Data-S_WAN_1 source S_Data destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_19
zone-pair security CSM_S_Data-W-S_POS_1 source S_Data-W destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_Data-W_S_POS
zone-pair security CSM_S_Data-W-S_POS-W_1 source S_Data-W destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_S_Data-W_S_POS-W
zone-pair security CSM_S_Data-W-S_WAN_1 source S_Data-W destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_19
zone-pair security CSM_S_Guest-S_POS_1 source S_Guest destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_Guest_S_POS
zone-pair security CSM_S_Guest-S_POS-W_1 source S_Guest destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_S_Guest_S_POS-W
zone-pair security CSM_S_Guest-S_WAN_1 source S_Guest destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_20
zone-pair security CSM_S_Partners-S_POS_1 source S_Partners destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_Partners_S_POS
zone-pair security CSM_S_Partners-S_POS-W_1 source S_Partners destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_MAP_10
zone-pair security CSM_S_Partners-S_WAN_1 source S_Partners destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_21
zone-pair security CSM_S_Voice-S_POS_1 source S_Voice destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_S_Voice_S_POS
zone-pair security CSM_S_Voice-S_POS-W_1 source S_Voice destination S_POS-W
 service-policy type inspect CSM_ZBF_POLICY_S_Voice_S_POS-W
zone-pair security CSM_S_Voice-S_WAN_1 source S_Voice destination S_WAN
 service-policy type inspect CSM_ZBF_POLICY_MAP_22
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.10.174.1 255.255.255.255
 ip pim sparse-dense-mode
 zone-member security LOOPBACK
!
interface FastEthernet0
 switchport mode trunk
!
interface FastEthernet1
 switchport access vlan 17
 switchport protected
!
interface FastEthernet2
 switchport access vlan 17
```

```
 switchport protected
!
interface FastEthernet3
 switchport access vlan 17
 switchport protected
!
interface FastEthernet4
 switchport access vlan 17
 switchport protected
!
interface FastEthernet5
 switchport access vlan 17
 switchport protected
!
interface FastEthernet6
 switchport access vlan 17
 switchport protected
!
interface FastEthernet7
 switchport access vlan 17
 switchport protected
!
interface FastEthernet8
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet8.1
!
interface GigabitEthernet0
 ip address 10.10.255.160 255.255.255.0
 ip ips Store-IPS in
 ip ips Store-IPS out
 zone-member security S_WAN
 duplex auto
 speed auto
 service-policy output BRANCH-WAN-EDGE
!
interface wlan-ap0
 description Service module interface to manage the embedded AP
 ip address 10.10.174.33 255.255.255.252
 zone-member security S_WLC-AP
 service-module ip address 10.10.174.34 255.255.255.252
 service-module ip default-gateway 10.10.174.33
 arp timeout 0
!
interface Wlan-GigabitEthernet0
 description Internal switch interface connecting to the embedded AP
 switchport mode trunk
 zone-member security S_WLC-AP
 service-module ip address 10.10.174.34 255.255.255.252
 service-module ip default-gateway 10.10.174.33
!
interface Vlan1
 no ip address
 ip ips Store-IPS in
 ip ips Store-IPS out
 zone-member security S_POS
!
interface Vlan11
 description POS
 ip address 10.10.160.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
```

```
 ip ips Store-IPS in
 ip ips Store-IPS out
 zone-member security S_POS
 standby 11 ip 10.10.160.1
 standby 11 priority 101
 standby 11 preempt
 ip igmp query-interval 125
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface Vlan12
 description DATA
 ip address 10.10.161.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip wccp 61 redirect in
 ip pim sparse-dense-mode
 zone-member security S_Data
 standby 12 ip 10.10.161.1
 standby 12 priority 101
 standby 12 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface Vlan13
 description VOICE
 ip address 10.10.162.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip pim sparse-dense-mode
 zone-member security S_Voice
 standby 13 ip 10.10.162.1
 standby 13 priority 101
 standby 13 preempt
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface Vlan14
 description WIRELESS
 ip address 10.10.163.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Data-W
 standby 14 ip 10.10.163.1
 standby 14 priority 101
 standby 14 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface Vlan15
 description WIRELESS-POS
 ip address 10.10.164.2 255.255.255.0
 ip helper-address 192.168.42.130
 ip ips Store-IPS in
 ip ips Store-IPS out
 zone-member security S_POS-W
 standby 15 ip 10.10.164.1
 standby 15 priority 101
 standby 15 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface Vlan16
 description PARTNER
 ip address 10.10.165.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Partners
 standby 16 ip 10.10.165.1
```

```
 standby 16 priority 101
 standby 16 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface Vlan17
 description WIRELESS-GUEST
 ip address 10.10.166.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Guest
 standby 17 ip 10.10.166.1
 standby 17 priority 101
 standby 17 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface Vlan18
 description WIRELESS-CONTROL
 ip address 10.10.167.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_WLC-AP
 standby 18 ip 10.10.167.1
 standby 18 priority 101
 standby 18 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface Vlan19
 description WAAS
 ip address 10.10.168.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_WAAS
 standby 19 ip 10.10.168.1
 standby 19 priority 101
 standby 19 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface Vlan20
 description SECURITY
 ip address 10.10.169.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_Security
 standby 20 ip 10.10.169.1
 standby 20 priority 101
 standby 20 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface Vlan21
 description HIPAA
 ip address 10.10.170.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_WAAS
 standby 19 ip 10.10.170.1
 standby 19 priority 101
 standby 19 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface Vlan22
 description WIRELESS-HIPAA-USERS
 ip address 10.10.171.2 255.255.255.0
 ip helper-address 192.168.42.130
```

```
 zone-member security S_WAAS
 standby 19 ip 10.10.171.1
 standby 19 priority 101
 standby 19 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface Vlan23
 description WIRELESS-HIPAA-DEVICES
 ip address 10.10.172.2 255.255.255.0
 ip helper-address 192.168.42.130
 zone-member security S_WAAS
 standby 19 ip 10.10.172.1
 standby 19 priority 101
 standby 19 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface Vlan1000
 description MANAGEMENT
 ip address 10.10.175.2 255.255.255.0
 zone-member security S_MGMT
 standby 100 ip 10.10.175.1
 standby 100 priority 101
 standby 100 preempt
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface Async1
 no ip address
 encapsulation slip
!
interface Group-Async0
 physical-layer async
 no ip address
 encapsulation slip
 no group-range
!
router ospf 5
 router-id 10.10.174.1
 passive-interface default
!
no ip forward-protocol nd
!
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication CiscoACS
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip route 0.0.0.0 0.0.0.0 10.10.255.11
ip tacacs source-interface Loopback0
!
ip access-list extended BULK-DATA-APPS
 remark ---File Transfer---
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
 remark ---E-mail traffic---
 permit tcp any any eq smtp
 permit tcp any any eq pop3
 permit tcp any any eq 143
 remark ---other EDM app protocols---
 permit tcp any any range 3460 3466
```

```
 permit tcp any range 3460 3466 any
 remark ---messaging services---
 permit tcp any any eq 2980
 permit tcp any eq 2980 any
 remark ---Microsoft file services---
 permit tcp any any range 137 139
 permit tcp any range 137 139 any
ip access-list extended CSM_ZBF_CMAP_ACL_1
 remark Data Center Mgmt to Devices
 permit object-group CSM_INLINE_svc_rule_68719541409 object-group
CSM_INLINE_src_rule_68719541409 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_10
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451205 object-group DC-POS-Oracle
object-group BRANCH-POS
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451209 object-group DC-POS-SAP object-group
BRANCH-POS
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451213 object-group DC-POS-Tomax
object-group BRANCH-POS
ip access-list extended CSM_ZBF_CMAP_ACL_11
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451215 object-group
CSM_INLINE_src_rule_73014451215 object-group BRANCH-POS
ip access-list extended CSM_ZBF_CMAP_ACL_12
 remark Data Center VOICE (wired and Wireless)
 permit object-group CSM_INLINE_svc_rule_68719541455 object-group DC-Voice object-group
Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_13
 remark Syslog and SNMP Alerts
 permit object-group CSM_INLINE_svc_rule_73014451187 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_73014451187
ip access-list extended CSM_ZBF_CMAP_ACL_14
 remark Store to Data Center Authentications
 permit object-group CSM_INLINE_svc_rule_73014451193 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_73014451193
ip access-list extended CSM_ZBF_CMAP_ACL_15
 remark Store to Data Center for NTP
 permit object-group NTP object-group Branches-ALL object-group NTP-Servers
ip access-list extended CSM_ZBF_CMAP_ACL_16
 remark Store to Data Center for DHCP and DNS
 permit object-group CSM_INLINE_svc_rule_73014451221 object-group Branches-ALL
object-group ActiveDirectory.cisco-irn.com
ip access-list extended CSM_ZBF_CMAP_ACL_17
 remark Permit ICMP traffic
 permit object-group CSM_INLINE_svc_rule_68719541425 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_68719541425
ip access-list extended CSM_ZBF_CMAP_ACL_18
 remark Store UCS E-series server to Data Center vShphere
 permit object-group CSM_INLINE_svc_rule_73014451197 object-group Branches-ALL
object-group vSphere-1
ip access-list extended CSM_ZBF_CMAP_ACL_19
 remark Store NAC
 permit object-group CSM_INLINE_svc_rule_73014451223 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_73014451223
ip access-list extended CSM_ZBF_CMAP_ACL_2
 remark Data Center subscribe to IPS SDEE events
 permit tcp object-group RSA-enVision object-group Branches-ALL eq 443
ip access-list extended CSM_ZBF_CMAP_ACL_20
 remark Store to Data Center Physical Security
 permit ip object-group Branches-ALL object-group CSM_INLINE_dst_rule_68719541435
ip access-list extended CSM_ZBF_CMAP_ACL_21
 remark Store WAAS (WAAS Devices need their own zone)
```

```
 permit object-group CSM_INLINE_svc_rule_68719541439 object-group Branches-ALL
object-group DC-WAAS
ip access-list extended CSM_ZBF_CMAP_ACL_22
 remark Store WAAS to Clients and Servers
 permit object-group CSM_INLINE_svc_rule_73014451388 object-group Branches-ALL
object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_23
 remark Store to Data Center wireless controller traffic
 permit object-group CSM_INLINE_svc_rule_68719541431 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_68719541431
ip access-list extended CSM_ZBF_CMAP_ACL_24
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451203 object-group BRANCH-POS object-group
DC-POS-Oracle
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451207 object-group BRANCH-POS object-group
DC-POS-SAP
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451211 object-group BRANCH-POS object-group
DC-POS-Tomax
ip access-list extended CSM_ZBF_CMAP_ACL_25
 remark Permit POS systems to talk to Data Center Servers
 permit object-group CSM_INLINE_svc_rule_73014451217 object-group
CSM_INLINE_src_rule_73014451217 object-group BRANCH-POS
ip access-list extended CSM_ZBF_CMAP_ACL_26
 remark Store to Data Center for E-mail
 permit object-group CSM_INLINE_svc_rule_73014451393 object-group BRANCH-POS object-group
MSExchange
ip access-list extended CSM_ZBF_CMAP_ACL_27
 remark Store to Data Center for Windows Updates
 permit object-group CSM_INLINE_svc_rule_73014451395 object-group BRANCH-POS object-group
MS-Update
ip access-list extended CSM_ZBF_CMAP_ACL_28
 remark Permit POS clients to talk to branch POS server
 permit object-group CSM_INLINE_svc_rule_73014451397 object-group BRANCH-POS object-group
BRANCH-POS
ip access-list extended CSM_ZBF_CMAP_ACL_29
 remark Store to Data Center for Windows Updates
 permit object-group CSM_INLINE_svc_rule_73014451404 object-group Branches-ALL
object-group MS-Update
ip access-list extended CSM_ZBF_CMAP_ACL_3
 remark Permit ICMP traffic
 permit object-group CSM_INLINE_svc_rule_68719541427 object-group
CSM_INLINE_src_rule_68719541427 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_30
 remark Store to Data Center for E-mail
 permit object-group CSM_INLINE_svc_rule_73014451406 object-group Branches-ALL
object-group MSExchange
ip access-list extended CSM_ZBF_CMAP_ACL_31
 remark Store DATA (wired and Wireless - Access to DC Other applications)
 permit object-group CSM_INLINE_svc_rule_68719541459 object-group Branches-ALL
object-group DC-Applications
ip access-list extended CSM_ZBF_CMAP_ACL_32
 remark Store GUEST - Drop Traffic to Enterprise
 permit ip object-group Branches-ALL object-group CSM_INLINE_dst_rule_68719541465
ip access-list extended CSM_ZBF_CMAP_ACL_33
 remark Store GUEST (access to internet/DMZ web servers)
 permit ip object-group Branches-ALL any
ip access-list extended CSM_ZBF_CMAP_ACL_34
 remark Store PARTNERS - Drop Traffic to Enterprise
 permit ip object-group Branches-ALL object-group CSM_INLINE_dst_rule_68719541461
ip access-list extended CSM_ZBF_CMAP_ACL_35
 remark Store PARTNERS (wired and wireless - Access to Partner site, Internet VPN)
 permit ip object-group Branches-ALL any
```

```
ip access-list extended CSM_ZBF_CMAP_ACL_36
 remark Store VOICE (wired and Wireless - Acess to corporate wide voice)
 permit object-group CSM_INLINE_svc_rule_68719541457 object-group Branches-ALL
object-group CSM_INLINE_dst_rule_68719541457
ip access-list extended CSM_ZBF_CMAP_ACL_4
 remark Data Center vSphere to UCS E-series server
 permit object-group CSM_INLINE_svc_rule_73014451195 object-group vSphere-1 object-group
Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_5
 remark Data Center to Store Physical Security
 permit ip object-group CSM_INLINE_src_rule_68719541433 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_6
 remark Data Center Mgmt to Devices
 permit object-group RDP object-group DC-Admin object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_7
 remark Data Center WAAS to Store
 permit object-group CSM_INLINE_svc_rule_68719541437 object-group
CSM_INLINE_src_rule_68719541437 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_8
 remark Data Center Wireless Control to AP's and Controllers in branchs
 permit object-group CSM_INLINE_svc_rule_68719541429 object-group
CSM_INLINE_src_rule_68719541429 object-group Branches-ALL
ip access-list extended CSM_ZBF_CMAP_ACL_9
 remark Data Center Mgmt to Devices
 permit object-group RDP object-group DC-Admin object-group BRANCH-POS
ip access-list extended MISSION-CRITICAL-SERVERS
 remark ---POS Applications---
 permit ip any 192.168.52.0 0.0.0.255
ip access-list extended NET-MGMT-APPS
 remark - Router user Authentication - Identifies TACACS Control traffic
 permit tcp any any eq tacacs
 permit tcp any eq tacacs any
ip access-list extended TRANSACTIONAL-DATA-APPS
 remark ---Workbrain Application---
 remark --Large Store Clock Server to Central Clock Application
 permit tcp host 10.10.49.94 host 192.168.46.72 eq 8444
 remark --Large branch Clock Server to CUAE
 permit tcp host 10.10.49.94 host 192.168.45.185 eq 8000
 remark ---LiteScape Application---
 permit ip any host 192.168.46.82
 permit ip any 239.192.0.0 0.0.0.255
 permit ip any host 239.255.255.250
 remark ---Remote Desktop---
 permit tcp any any eq 3389
 permit tcp any eq 3389 any
 remark ---Oracle SIM---
 permit tcp any 192.168.46.0 0.0.0.255 eq 7777
 permit tcp any 192.168.46.0 0.0.0.255 eq 6003
 permit tcp any 192.168.46.0 0.0.0.255 range 12401 12500
 permit tcp 192.168.46.0 0.0.0.255 eq 7777 any
 permit tcp 192.168.46.0 0.0.0.255 eq 6003 any
 permit tcp 192.168.46.0 0.0.0.255 range 12401 12500 any
!
logging esm config
logging trap debugging
logging source-interface Loopback0
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
```

```
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
!
!
!
!
!
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group causer v3 priv
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps flash insertion removal
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps energywise
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps ipsla
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server domain-stripping
tacacs-server key 7 <removed>
!
!
control-plane
!
banner exec C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner incoming C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
```

```
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

banner login C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!

!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication CiscoACS
line 1
 modem InOut
 stopbits 1
 speed 115200
 flowcontrol hardware
line 2
 no activation-character
 no exec
 transport preferred none
 transport input ssh
 transport output none
line aux 0
 session-timeout 1  output
 exec-timeout 0 1
 privilege level 0
 login authentication CiscoACS
 no exec
 transport preferred none
 transport output none
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
!
scheduler max-task-time 5000
ntp source Loopback0
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162
end
```

S-A2-CONV-1

```
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname S-A2-Conv-1
!
boot-start-marker
boot-end-marker
!
logging buffered 50000
enable secret 5 <removed>
!

username bart privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
!
aaa new-model
!
!
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
system mtu routing 1500
!
!
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
password encryption aes
!
crypto pki trustpoint TP-self-signed-3179870208
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3179870208
 revocation-check none
 rsakeypair TP-self-signed-3179870208
!
!
crypto pki certificate chain TP-self-signed-3179870208
 certificate self-signed 01
  <removed>
  quit
```

```
!
!
!
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip ssh version 2
ip scp server enable
!
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
 description AIR-CAP1042N
 switchport trunk native vlan 18
 switchport trunk allowed vlan 14-18
 switchport mode trunk
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface GigabitEthernet0/1
 switchport mode trunk
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan1000
 description Management VLAN for Switch
 ip address 10.10.175.11 255.255.255.0
 no ip route-cache
!
ip default-gateway 10.10.175.1
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication CiscoACS
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Vlan1000
!
ip sla enable reaction-alerts
logging trap debugging
logging source-interface Vlan1000
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
```

```
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access  88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFF0F
snmp-server trap-source Vlan1000
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps power-ethernet group 1
snmp-server enable traps power-ethernet police
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps energywise
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131 timeout 5
tacacs-server directed-request
tacacs-server key 7 <removed>
banner exec ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                  **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
```

```
                    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication CiscoACS
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
!
ntp clock-period 36028799
ntp source Vlan1000
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end
```

Managed Service Provider

FW-A2-MSP-1

```
ASA Version 9.0(0)129
!
terminal width 511
hostname FW-A2-MSP-1
domain-name cisco-irn.com
enable password <removed> encrypted
passwd <removed> encrypted
names
dns-guard
```

```
!
interface GigabitEthernet0/0
 nameif MSP-WAN
 security-level 0
 ip address 10.10.255.176 255.255.255.0
!
interface GigabitEthernet0/1
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/1.11
 vlan 11
 nameif POS
 security-level 95
 ip address 10.10.176.1 255.255.255.0
!
interface GigabitEthernet0/1.12
 vlan 12
 nameif DATA
 security-level 85
 ip address 10.10.177.1 255.255.255.0
!
interface GigabitEthernet0/1.13
 vlan 13
 nameif VOICE
 security-level 80
 ip address 10.10.178.1 255.255.255.0
!
interface GigabitEthernet0/1.14
 vlan 14
 nameif WIRELESS
 security-level 70
 ip address 10.10.179.1 255.255.255.0
!
interface GigabitEthernet0/1.15
 vlan 15
 nameif WIRELESS-POS
 security-level 90
 ip address 10.10.180.1 255.255.255.0
!
interface GigabitEthernet0/1.16
 vlan 16
 nameif PARTNER
 security-level 65
 ip address 10.10.181.1 255.255.255.0
!
interface GigabitEthernet0/1.17
 vlan 17
 nameif WIRELESS-GUEST
 security-level 10
 ip address 10.10.182.1 255.255.255.0
!
interface GigabitEthernet0/1.18
 vlan 18
 nameif WIRELESS-CONTROL
 security-level 75
 ip address 10.10.183.1 255.255.255.0
!
interface GigabitEthernet0/1.19
 vlan 19
 nameif WAAS
 security-level 100
 ip address 10.10.184.1 255.255.255.0
```

```
!
interface GigabitEthernet0/1.21
 vlan 21
 nameif HIPAA
 security-level 95
 ip address 10.10.184.1 255.255.255.0
!
interface GigabitEthernet0/1.22
 vlan 22
 nameif WIRELESS-HIPAA-USERS
 security-level 85
 ip address 10.10.184.1 255.255.255.0
!
interface GigabitEthernet0/1.23
 vlan 23
 nameif WIRELESS-HIPAA-DEVICES
 security-level 75
 ip address 10.10.184.1 255.255.255.0
!
interface GigabitEthernet0/1.1000
 vlan 1000
 nameif MANAGEMENT
 security-level 100
 ip address 10.10.191.1 255.255.255.0
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 description IPS management connection
 management-only
 nameif IPS-Mgmt
 security-level 1
 no ip address
!
banner exec WARNING:
banner exec **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
banner exec                                **** AUTHORIZED USERS ONLY! ****
banner exec
banner exec ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
banner exec TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE
NECESSARY
banner exec TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
```

```
banner exec REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME
WITHOUT
banner exec FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
banner exec CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
banner exec ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
banner exec
banner exec UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL
LAWS.
banner login WARNING:
banner login THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
banner asdm WARNING:
banner asdm   **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
banner asdm                   **** AUTHORIZED USERS ONLY! ****
banner asdm
banner asdm ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY TO
IDENTIFY ANY UNAUTHORIZED USER. THE SYSTEM ADMINISTRATOR OR OTHER REPRESENTATIVES OF T
HE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT FURTHER NOTICE OR CONSENT.
UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER CRIMINAL CONDUCT REVEALED BY SUCH USE IS
SUBJECT TO DISCLOSURE TO LAW ENFORCEMENT OFFICIALS AND PROSECUTION TO THE F
banner asdm
banner asdm UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL
LAWS
boot system disk0:/asa900-129-smp-k8.bin
ftp mode passive
clock timezone PST -8
clock summer-time PDT recurring
dns domain-lookup MSP-WAN
dns server-group DefaultDNS
 name-server 192.168.42.130
 domain-name cisco-irn.com
same-security-traffic permit inter-interface
object network AdminStation
 host 192.168.41.101
object network AdminStation2
 host 192.168.41.102
object network AdminStation4-bart
 host 10.19.151.99
object network LMS
 host 192.168.42.139
object network CSManager
 host 192.168.42.133
 description Cisco Security Manager
object network AdminStation3
 host 192.168.42.139
object network ActiveDirectory.cisco-irn.com
 host 192.168.42.130
object network DC-POS
 subnet 192.168.52.0 255.255.255.0
 description POS in the Data Center
object network WCSManager
 host 192.168.43.135
 description Wireless Manager
object network PAME-DC-1
 host 192.168.44.111
object network MSP-DC-1
 host 192.168.44.121
 description Data Center VSOM
object network DC-ALL
 subnet 192.168.0.0 255.255.0.0
 description All of the Data Center
object network RSA-enVision
 host 192.168.42.124
 description RSA EnVision Syslog collector and SIM
```

```
object network TACACS
 host 192.168.42.131
 description Csico Secure ACS server for TACACS and Radius
object network RSA-AM
 host 192.168.42.137
 description RSA Authentication Manager for SecureID
object network NAC-2
 host 192.168.42.112
object network NAC-1
 host 192.168.42.111
 description ISE server for NAC
object network MS-Update
 host 192.168.42.150
 description Windows Update Server
object network MSExchange
 host 192.168.42.140
 description Mail Server
object service RPC
 service tcp destination eq 135
object service LDAP-GC
 service tcp destination eq 3268
object service LDAP-GC-SSL
 service tcp destination eq 3269
object service Kerberos-TCP
 service tcp destination eq 88
object service Microsoft-DS-SMB
 service tcp destination eq 445
 description Microsoft-DS Active Directory, Windows shares Microsoft-DS SMB file sharing
object service LDAP-UDP
 service udp destination eq 389
object service RPC-HighPorts
 service tcp destination range 1024 65535
object service ORACLE-OAS
 service tcp destination eq 12601
 description OAS uses one port for HTTP and RMI - 12601.
object service TOMAX-8990
 service tcp destination eq 8990
 description Tomax Application Port
object service IP-Protocol-97
 service 97
 description IP protocol 97
object service TCP1080
 service tcp destination eq 1080
object service TCP8080
 service tcp destination eq 8080
object service RDP
 service tcp destination eq 3389
 description Windows Remote Desktop
object-group network CSM_INLINE_src_rule_73014461090
 description Generated by CS-Manager from src of FirewallRule# 1 (ASA-Store_V2/mandatory)
 network-object object AdminStation
 network-object object AdminStation2
 network-object object AdminStation4-bart
object-group network Admin-Systems
 network-object object AdminStation
 network-object object AdminStation2
 network-object object CSManager
 network-object object AdminStation4-bart
 network-object object LMS
 network-object object AdminStation3
object-group network DC-POS-Tomax
 description Tomax POS Communication from Store to Data Center
 network-object 192.168.52.96 255.255.255.224
object-group network DC-POS-SAP
```

```
 description SAP POS Communication from Store to Data Center
 network-object 192.168.52.144 255.255.255.240
object-group network DC-POS-Oracle
 description Oracle POS Communication from Store to Data Center
 network-object 192.168.52.128 255.255.255.240
object-group network CSM_INLINE_src_rule_73014461184
 description Generated by CS-Manager from src of FirewallRule# 4 (ASA-Store_V2/mandatory)
 group-object DC-POS-Tomax
 network-object object DC-POS
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
object-group network POS-Store-MSP
 network-object 10.10.176.81 255.255.255.255
object-group network CSM_INLINE_dst_rule_73014461438
 description Generated by CS-Manager from dst of FirewallRule# 5 (ASA-Store_V2/mandatory)
 group-object DC-POS-Tomax
 network-object object DC-POS
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
object-group network Store-MSP-POS-net
 network-object 10.10.176.0 255.255.255.0
 network-object 10.10.180.0 255.255.255.0
object-group network CSM_INLINE_dst_rule_73014461436
 description Generated by CS-Manager from dst of FirewallRule# 7 (ASA-Store_V2/mandatory)
 group-object DC-POS-Tomax
 network-object object DC-POS
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
object-group network DC-Wifi-Controllers
 description Central Wireless Controllers for branchs
 network-object 192.168.43.21 255.255.255.255
 network-object 192.168.43.22 255.255.255.255
object-group network DC-Wifi-MSE
 description Mobility Service Engines
 network-object 192.168.43.31 255.255.255.255
 network-object 192.168.43.32 255.255.255.255
object-group network CSM_INLINE_src_rule_73014461098
 description Generated by CS-Manager from src of FirewallRule# 8 (ASA-Store_V2/mandatory)
 network-object object WCSManager
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
object-group network CSM_INLINE_src_rule_73014461100
 description Generated by CS-Manager from src of FirewallRule# 9 (ASA-Store_V2/mandatory)
 network-object object PAME-DC-1
 network-object object MSP-DC-1
object-group network DC-WAAS
 description WAE Appliances in Data Center
 network-object 192.168.48.10 255.255.255.255
 network-object 192.168.49.10 255.255.255.255
 network-object 192.168.47.11 255.255.255.255
 network-object 192.168.47.12 255.255.255.255
object-group network NTP-Servers
 description NTP Servers
 network-object 192.168.62.161 255.255.255.255
 network-object 162.168.62.162 255.255.255.255
object-group network CSM_INLINE_dst_rule_73014461120
 description Generated by CS-Manager from dst of FirewallRule# 17 (ASA-Store_V2/mandatory)
 network-object object TACACS
 network-object object RSA-AM
 network-object object NAC-2
 network-object object NAC-1
object-group network CSM_INLINE_dst_rule_73014461126
 description Generated by CS-Manager from dst of FirewallRule# 18 (ASA-Store_V2/mandatory)
 network-object object PAME-DC-1
```

```
 network-object object MSP-DC-1
object-group network CSM_INLINE_dst_rule_73014461128
 description Generated by CS-Manager from dst of FirewallRule# 19 (ASA-Store_V2/mandatory)
 group-object DC-Wifi-Controllers
 group-object DC-Wifi-MSE
object-group service HTTPS-8443
 service-object tcp destination eq 8443
object-group service CSM_INLINE_svc_rule_73014461092
 description Generated by CS-Manager from service of FirewallRule# 2
(ASA-Store_V2/mandatory)
 service-object tcp destination eq ssh
 service-object tcp destination eq https
 group-object HTTPS-8443
 service-object udp destination eq snmp
object-group service DNS-Resolving
 description Domain Name Server
 service-object tcp destination eq domain
 service-object udp destination eq domain
object-group service CSM_INLINE_svc_rule_73014461094
 description Generated by CS-Manager from service of FirewallRule# 3
(ASA-Store_V2/mandatory)
 service-object tcp destination eq ldap
 service-object tcp destination eq ldaps
 service-object udp destination eq 88
 service-object udp destination eq ntp
 service-object udp destination eq netbios-dgm
 service-object object RPC
 service-object object LDAP-GC
 service-object object LDAP-GC-SSL
 service-object object Kerberos-TCP
 service-object object Microsoft-DS-SMB
 service-object object LDAP-UDP
 service-object object RPC-HighPorts
 group-object DNS-Resolving
object-group service ORACLE-RMI
 description RMI TCP ports 1300 and 1301-1319.
 service-object tcp destination range 1300 1319
object-group service ORACLE-Weblogic
 description HTTP/RMI and HTTPS/RMI-SSL 7001 & 7002. OracleAQ uses 1521.
 service-object tcp destination eq 7001
 service-object tcp destination eq 7002
 service-object tcp destination eq sqlnet
object-group service ORACLE-WAS
 description RMI/IIOP over 2809  HTTP over 9443 IBM-MQ 1414
 service-object tcp destination eq 2809
 service-object tcp destination eq 9443
 service-object tcp destination eq 1414
object-group service CSM_INLINE_svc_rule_73014461184
 description Generated by CS-Manager from service of FirewallRule# 4
(ASA-Store_V2/mandatory)
 service-object tcp destination eq https
 service-object tcp destination eq ssh
 service-object object ORACLE-OAS
 service-object object TOMAX-8990
 group-object ORACLE-RMI
 group-object ORACLE-Weblogic
 group-object ORACLE-WAS
 group-object HTTPS-8443
object-group service TFTP
 description Trivial File Transfer
 service-object tcp destination eq 69
 service-object udp destination eq tftp
object-group service LWAPP
 description LWAPP UDP ports 12222 and 12223
```

```
 service-object udp destination eq 12222
 service-object udp destination eq 12223
object-group service CAPWAP
 description CAPWAP UDP ports 5246 and 5247
 service-object udp destination eq 5246
 service-object udp destination eq 5247
object-group service CSM_INLINE_svc_rule_73014461098
 description Generated by CS-Manager from service of FirewallRule# 8
(ASA-Store_V2/mandatory)
 service-object tcp destination eq https
 service-object tcp destination eq www
 service-object udp destination eq isakmp
 service-object tcp destination eq telnet
 service-object tcp destination eq ssh
 service-object object IP-Protocol-97
 group-object TFTP
 group-object LWAPP
 group-object CAPWAP
object-group service CSM_INLINE_svc_rule_73014461102
 description Generated by CS-Manager from service of FirewallRule# 10
(ASA-Store_V2/mandatory)
 service-object icmp echo
 service-object icmp echo-reply
 service-object tcp destination eq www
 service-object tcp destination eq https
 service-object tcp destination eq ssh
 service-object tcp destination eq ftp
 service-object object TCP1080
 service-object object TCP8080
 service-object object RDP
 group-object HTTPS-8443
object-group service CISCO-WAAS
 description Ports for Cisco WAAS
 service-object tcp destination eq 4050
object-group service Netbios
 description Netbios Servers
 service-object udp destination eq netbios-dgm
 service-object udp destination eq netbios-ns
 service-object tcp destination eq netbios-ssn
object-group service CSM_INLINE_svc_rule_73014461104
 description Generated by CS-Manager from service of FirewallRule# 11
(ASA-Store_V2/mandatory)
 service-object object Microsoft-DS-SMB
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Netbios
object-group service CSM_INLINE_svc_rule_73014461106
 description Generated by CS-Manager from service of FirewallRule# 12
(ASA-Store_V2/mandatory)
 service-object tcp-udp destination eq sip
 service-object tcp destination eq 2000
object-group service CSM_INLINE_svc_rule_73014461112
 description Generated by CS-Manager from service of FirewallRule# 14
(ASA-Store_V2/mandatory)
 service-object udp destination eq snmptrap
 service-object udp destination eq snmp
 service-object udp destination eq syslog
object-group service CSM_INLINE_svc_rule_73014461120
 description Generated by CS-Manager from service of FirewallRule# 17
(ASA-Store_V2/mandatory)
 service-object udp destination eq 1812
 service-object udp destination eq 1813
 service-object tcp destination eq https
 service-object tcp destination eq www
```

```
 group-object HTTPS-8443
object-group service Cisco-Mobility
 description Mobility ports for Wireless
 service-object udp destination eq 16666
 service-object udp destination eq 16667
object-group service CSM_INLINE_svc_rule_73014461128
 description Generated by CS-Manager from service of FirewallRule# 19
(ASA-Store_V2/mandatory)
 service-object tcp destination eq https
 service-object udp destination eq isakmp
 service-object object IP-Protocol-97
 group-object Cisco-Mobility
 group-object LWAPP
 group-object CAPWAP
object-group service CSM_INLINE_svc_rule_73014461130
 description Generated by CS-Manager from service of FirewallRule# 20
(ASA-Store_V2/mandatory)
 service-object tcp-udp destination eq sip
 service-object tcp destination eq 2000
object-group service CSM_INLINE_svc_rule_73014461132
 description Generated by CS-Manager from service of FirewallRule# 21
(ASA-Store_V2/mandatory)
 service-object object Microsoft-DS-SMB
 group-object CISCO-WAAS
 group-object HTTPS-8443
 group-object Netbios
object-group service CSM_INLINE_svc_rule_73014461134
 description Generated by CS-Manager from service of FirewallRule# 22
(ASA-Store_V2/mandatory)
 service-object tcp destination eq ldap
 service-object tcp destination eq ldaps
 service-object udp destination eq 88
 service-object udp destination eq ntp
 service-object udp destination eq netbios-dgm
 service-object object RPC
 service-object object LDAP-GC
 service-object object LDAP-GC-SSL
 service-object object Kerberos-TCP
 service-object object Microsoft-DS-SMB
 service-object object LDAP-UDP
 service-object object RPC-HighPorts
 group-object DNS-Resolving
object-group service CSM_INLINE_svc_rule_73014461136
 description Generated by CS-Manager from service of FirewallRule# 23
(ASA-Store_V2/mandatory)
 service-object tcp destination eq www
 service-object tcp destination eq https
object-group service CSM_INLINE_svc_rule_73014461138
 description Generated by CS-Manager from service of FirewallRule# 24
(ASA-Store_V2/mandatory)
 service-object tcp destination eq www
 service-object tcp destination eq https
 service-object tcp destination eq smtp
 service-object tcp destination eq pop3
 service-object tcp destination eq imap4
object-group network DM_INLINE_NETWORK_2
 network-object object NAC-1
 network-object object NAC-2
 network-object object TACACS
object-group service DM_INLINE_SERVICE_1
 service-object icmp6 echo
 service-object udp destination eq ntp
object-group service DM_INLINE_SERVICE_2
 service-object icmp echo
```

```
 service-object tcp destination eq tacacs
object-group service DM_INLINE_SERVICE_3
 service-object icmp echo
 service-object udp destination eq radius
 service-object udp destination eq radius-acct
object-group service DM_INLINE_SERVICE_4
 service-object icmp echo
 service-object udp destination eq snmp
 service-object udp destination eq snmptrap
 service-object udp destination eq syslog
object-group network DM_INLINE_NETWORK_3
 network-object object LMS
 network-object object RSA-enVision
access-list OUTSIDE remark LAB Testing
access-list OUTSIDE extended permit ip object-group CSM_INLINE_src_rule_73014461090
10.10.176.0 255.255.248.0
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_73014461092
object-group Admin-Systems 10.10.176.0 255.255.24
8.0
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_73014461092
object-group Admin-Systems host 10.10.255.176
access-list OUTSIDE remark Allow Active Directory Domain
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_73014461094 object
ActiveDirectory.cisco-irn.com 10.10.176.0
255.255.248.0
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_73014461184
object-group CSM_INLINE_src_rule_73014461184 obje
ct-group POS-Store-MSP
access-list OUTSIDE extended deny ip any object-group Store-MSP-POS-net
access-list OUTSIDE extended deny ip any object-group CSM_INLINE_dst_rule_73014461436
access-list OUTSIDE remark Wireless Management to Stores
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_73014461098
object-group CSM_INLINE_src_rule_73014461098 10.1
0.183.0 255.255.255.0
access-list OUTSIDE remark Physical security systems
access-list OUTSIDE extended permit tcp object-group CSM_INLINE_src_rule_73014461100
10.10.191.0 255.255.255.0 eq https
access-list OUTSIDE remark Allow Management of branch systems
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_73014461102 object
DC-ALL 10.10.176.0 255.255.248.0
access-list OUTSIDE remark WAAS systems
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_73014461104
object-group DC-WAAS 10.10.184.0 255.255.255.0
access-list OUTSIDE remark Voice calls
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_73014461106 object
DC-ALL 10.10.178.0 255.255.255.0
access-list OUTSIDE extended permit tcp 10.10.176.0 255.255.248.0 object LMS eq ssh
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_73014461112
10.10.176.0 255.255.248.0 object RSA-enVision
access-list OUTSIDE extended permit tcp 10.10.176.0 255.255.248.0 object TACACS eq tacacs
access-list OUTSIDE extended permit udp 10.10.176.0 255.255.248.0 object-group NTP-Servers
eq ntp
access-list OUTSIDE remark Drop all other traffic
access-list OUTSIDE extended deny ip any any log
access-list POS remark Allow Applications
access-list POS extended permit tcp object-group POS-Store-MSP object-group
CSM_INLINE_dst_rule_73014461438 eq https
access-list POS extended deny ip any object-group Store-MSP-POS-net
access-list POS extended deny ip any object-group CSM_INLINE_dst_rule_73014461436
access-list POS extended permit udp 10.10.176.0 255.255.248.0 object-group NTP-Servers eq
ntp
access-list POS extended permit object-group CSM_INLINE_svc_rule_73014461120 10.10.176.0
255.255.248.0 object-group CSM_INLINE_dst
_rule_73014461120
```

```
access-list POS remark Allow Active Directory Domain
access-list POS extended permit object-group CSM_INLINE_svc_rule_73014461134 10.10.176.0
255.255.248.0 object ActiveDirectory.cisc
o-irn.com
access-list POS remark Allow Windows Updates
access-list POS extended permit object-group CSM_INLINE_svc_rule_73014461136 10.10.176.0
255.255.248.0 object MS-Update
access-list POS remark Allow Mail
access-list POS extended permit object-group CSM_INLINE_svc_rule_73014461138 10.10.176.0
255.255.248.0 object MSExchange
access-list POS remark Drop all other traffic
access-list POS extended deny ip any any log
access-list WIRELESS-POS remark Allow Applications
access-list WIRELESS-POS extended permit tcp object-group POS-Store-MSP object-group
CSM_INLINE_dst_rule_73014461438 eq https
access-list WIRELESS-POS extended deny ip any object-group Store-MSP-POS-net
access-list WIRELESS-POS extended deny ip any object-group CSM_INLINE_dst_rule_73014461436
access-list WIRELESS-POS extended permit udp 10.10.176.0 255.255.248.0 object-group
NTP-Servers eq ntp
access-list WIRELESS-POS remark Allow Active Directory Domain
access-list WIRELESS-POS extended permit object-group CSM_INLINE_svc_rule_73014461134
10.10.176.0 255.255.248.0 object ActiveDirectory.cisco-irn.com
access-list WIRELESS-POS remark Allow Windows Updates
access-list WIRELESS-POS extended permit object-group CSM_INLINE_svc_rule_73014461136
10.10.176.0 255.255.248.0 object MS-Update
access-list WIRELESS-POS remark Allow Mail
access-list WIRELESS-POS extended permit object-group CSM_INLINE_svc_rule_73014461138
10.10.176.0 255.255.248.0 object MSExchange
access-list WIRELESS-POS remark Drop all other traffic
access-list WIRELESS-POS extended deny ip any any log
access-list DATA extended deny ip any object-group Store-MSP-POS-net
access-list DATA extended deny ip any object-group CSM_INLINE_dst_rule_73014461436
access-list DATA extended permit udp 10.10.176.0 255.255.248.0 object-group NTP-Servers eq
ntp
access-list DATA extended permit object-group CSM_INLINE_svc_rule_73014461120 10.10.176.0
255.255.248.0 object-group CSM_INLINE_dst_rule_73014461120
access-list DATA remark Allow Active Directory Domain
access-list DATA extended permit object-group CSM_INLINE_svc_rule_73014461134 10.10.176.0
255.255.248.0 object ActiveDirectory.cisco-irn.com
access-list DATA remark Allow Windows Updates
access-list DATA extended permit object-group CSM_INLINE_svc_rule_73014461136 10.10.176.0
255.255.248.0 object MS-Update
access-list DATA remark Allow Mail
access-list DATA extended permit object-group CSM_INLINE_svc_rule_73014461138 10.10.176.0
255.255.248.0 object MSExchange
access-list DATA remark Drop all other traffic
access-list DATA extended deny ip any any log
access-list MANAGEMENT extended deny ip any object-group Store-MSP-POS-net
access-list MANAGEMENT extended deny ip any object-group CSM_INLINE_dst_rule_73014461436
access-list MANAGEMENT extended permit tcp 10.10.176.0 255.255.248.0 object LMS eq ssh
access-list MANAGEMENT extended permit object-group CSM_INLINE_svc_rule_73014461112
10.10.176.0 255.255.248.0 object RSA-enVision
access-list MANAGEMENT extended permit tcp 10.10.176.0 255.255.248.0 object TACACS eq
tacacs
access-list MANAGEMENT extended permit udp 10.10.176.0 255.255.248.0 object-group
NTP-Servers eq ntp
access-list MANAGEMENT extended permit icmp 10.10.176.0 255.255.248.0 object-group
NTP-Servers
access-list MANAGEMENT extended permit object-group CSM_INLINE_svc_rule_73014461120
10.10.176.0 255.255.248.0 object-group CSM_INLINE_dst_rule_73014461120
access-list MANAGEMENT remark Physical security systems
access-list MANAGEMENT extended permit tcp 10.10.191.0 255.255.255.0 object-group
CSM_INLINE_dst_rule_73014461126 eq https
access-list MANAGEMENT remark Allow Mail
```

```
access-list MANAGEMENT extended permit object-group CSM_INLINE_svc_rule_73014461138
10.10.176.0 255.255.248.0 object MSExchange
access-list MANAGEMENT remark Drop all other traffic
access-list MANAGEMENT extended deny ip any any log
access-list PARTNER extended deny ip any object-group Store-MSP-POS-net
access-list PARTNER extended deny ip any object-group CSM_INLINE_dst_rule_73014461436
access-list PARTNER extended permit udp 10.10.176.0 255.255.248.0 object-group NTP-Servers
eq ntp
access-list PARTNER extended permit object-group CSM_INLINE_svc_rule_73014461120
10.10.176.0 255.255.248.0 object-group CSM_INLINE_dst_rule_73014461120
access-list PARTNER remark Allow Mail
access-list PARTNER extended permit object-group CSM_INLINE_svc_rule_73014461138
10.10.176.0 255.255.248.0 object MSExchange
access-list PARTNER remark Drop all other traffic
access-list PARTNER extended deny ip any any log
access-list VOICE extended deny ip any object-group Store-MSP-POS-net
access-list VOICE extended deny ip any object-group CSM_INLINE_dst_rule_73014461436
access-list VOICE extended permit tcp 10.10.176.0 255.255.248.0 object LMS eq ssh
access-list VOICE extended permit object-group CSM_INLINE_svc_rule_73014461112 10.10.176.0
255.255.248.0 object RSA-enVision
access-list VOICE extended permit tcp 10.10.176.0 255.255.248.0 object TACACS eq tacacs
access-list VOICE extended permit udp 10.10.176.0 255.255.248.0 object-group NTP-Servers
eq ntp
access-list VOICE extended permit object-group CSM_INLINE_svc_rule_73014461120 10.10.176.0
255.255.248.0 object-group CSM_INLINE_dst_rule_73014461120
access-list VOICE remark Voice calls
access-list VOICE extended permit object-group CSM_INLINE_svc_rule_73014461130 10.10.178.0
255.255.255.0 object DC-ALL
access-list VOICE remark Allow Mail
access-list VOICE extended permit object-group CSM_INLINE_svc_rule_73014461138 10.10.176.0
255.255.248.0 object MSExchange
access-list VOICE remark Drop all other traffic
access-list VOICE extended deny ip any any log
access-list WAAS extended deny ip any object-group Store-MSP-POS-net
access-list WAAS extended deny ip any object-group CSM_INLINE_dst_rule_73014461436
access-list WAAS extended permit tcp 10.10.176.0 255.255.248.0 object LMS eq ssh
access-list WAAS extended permit object-group CSM_INLINE_svc_rule_73014461112 10.10.176.0
255.255.248.0 object RSA-enVision
access-list WAAS extended permit tcp 10.10.176.0 255.255.248.0 object TACACS eq tacacs
access-list WAAS extended permit udp 10.10.176.0 255.255.248.0 object-group NTP-Servers eq
ntp
access-list WAAS remark WAAS systems
access-list WAAS extended permit object-group CSM_INLINE_svc_rule_73014461132 10.10.184.0
255.255.255.0 object-group DC-WAAS
access-list WAAS remark Allow Active Directory Domain
access-list WAAS extended permit object-group CSM_INLINE_svc_rule_73014461134 10.10.176.0
255.255.248.0 object ActiveDirectory.cisco-irn.com
access-list WAAS remark Drop all other traffic
access-list WAAS extended deny ip any any log
access-list WIRELESS extended deny ip any object-group Store-MSP-POS-net
access-list WIRELESS extended deny ip any object-group CSM_INLINE_dst_rule_73014461436
access-list WIRELESS extended permit udp 10.10.176.0 255.255.248.0 object-group
NTP-Servers eq ntp
access-list WIRELESS remark Allow Active Directory Domain
access-list WIRELESS extended permit object-group CSM_INLINE_svc_rule_73014461134
10.10.176.0 255.255.248.0 object ActiveDirectory.cisco-irn.com
access-list WIRELESS remark Allow Windows Updates
access-list WIRELESS extended permit object-group CSM_INLINE_svc_rule_73014461136
10.10.176.0 255.255.248.0 object MS-Update
access-list WIRELESS remark Allow Mail
access-list WIRELESS extended permit object-group CSM_INLINE_svc_rule_73014461138
10.10.176.0 255.255.248.0 object MSExchange
access-list WIRELESS remark Drop all other traffic
access-list WIRELESS extended deny ip any any log
```

```
access-list WIRELESS-CONTROL extended deny ip any object-group Store-MSP-POS-net
access-list WIRELESS-CONTROL extended deny ip any object-group
CSM_INLINE_dst_rule_73014461436
access-list WIRELESS-CONTROL extended permit tcp 10.10.176.0 255.255.248.0 object LMS eq
ssh
access-list WIRELESS-CONTROL extended permit object-group CSM_INLINE_svc_rule_73014461112
10.10.176.0 255.255.248.0 object RSA-enVision
access-list WIRELESS-CONTROL extended permit tcp 10.10.176.0 255.255.248.0 object TACACS
eq tacacs
access-list WIRELESS-CONTROL extended permit udp 10.10.176.0 255.255.248.0 object-group
NTP-Servers eq ntp
access-list WIRELESS-CONTROL extended permit object-group CSM_INLINE_svc_rule_73014461120
10.10.176.0 255.255.248.0 object-group CSM_INLINE_dst_rule_73014461120
access-list WIRELESS-CONTROL remark Wireless control systems
access-list WIRELESS-CONTROL extended permit object-group CSM_INLINE_svc_rule_73014461128
10.10.183.0 255.255.255.0 object-group CSM_INLINE_dst_rule_73014461128
access-list WIRELESS-CONTROL remark Drop all other traffic
access-list WIRELESS-CONTROL extended deny ip any any log
access-list WIRELESS-GUEST extended deny ip any object-group Store-MSP-POS-net
access-list WIRELESS-GUEST extended deny ip any object-group
CSM_INLINE_dst_rule_73014461436
access-list WIRELESS-GUEST extended permit udp 10.10.176.0 255.255.248.0 object-group
NTP-Servers eq ntp
access-list WIRELESS-GUEST remark Drop all other traffic
access-list WIRELESS-GUEST extended deny ip any any log
access-list DROP-ALL extended deny ip any any log disable
access-list MANAGEMENT_access_in extended permit object-group DM_INLINE_SERVICE_1
10.10.191.0 255.255.255.0 object-group NTP-Servers log disable
access-list MANAGEMENT_access_in extended permit object-group DM_INLINE_SERVICE_2
10.10.191.0 255.255.255.0 object TACACS
access-list MANAGEMENT_access_in extended permit object-group DM_INLINE_SERVICE_3
10.10.191.0 255.255.255.0 object-group DM_INLINE_NETWORK_2 log disable
access-list MANAGEMENT_access_in extended permit object-group DM_INLINE_SERVICE_4
10.10.191.0 255.255.255.0 object-group DM_INLINE_NETWORK_3 log disable
access-list MANAGEMENT_access_in extended deny ip any any
pager lines 24
logging enable
logging timestamp
logging buffer-size 100000
logging trap informational
logging asdm informational
logging host MSP-WAN 192.168.42.124
mtu MSP-WAN 1500
mtu POS 1500
mtu DATA 1500
mtu VOICE 1500
mtu WIRELESS 1500
mtu WIRELESS-POS 1500
mtu PARTNER 1500
mtu WIRELESS-GUEST 1500
mtu WIRELESS-CONTROL 1500
mtu WAAS 1500
mtu HIPAA 1500
mtu WIRELESS-HIPAA-USERS 1500
mtu WIRELESS-HIPAA-DEVICES 1500
mtu MANAGEMENT 1500
mtu IPS-Mgmt 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
icmp permit any MSP-WAN
icmp permit any POS
icmp permit any DATA
icmp permit any VOICE
icmp permit any WIRELESS
```

```
icmp permit any WIRELESS-POS
icmp permit any PARTNER
icmp permit any WIRELESS-GUEST
icmp permit any WIRELESS-CONTROL
icmp permit any WAAS
icmp permit any HIPAA
icmp permit any WIRELESS-HIPAA-USERS
icmp permit any WIRELESS-HIPAA-DEVICES
icmp permit any MANAGEMENT
asdm image disk0:/asdm-70040.bin
asdm history enable
arp timeout 14400
no arp permit-nonconnected
access-group OUTSIDE in interface MSP-WAN
access-group POS in interface POS
access-group DATA in interface DATA
access-group VOICE in interface VOICE
access-group WIRELESS in interface WIRELESS
access-group WIRELESS-POS in interface WIRELESS-POS
access-group PARTNER in interface PARTNER
access-group WIRELESS-GUEST in interface WIRELESS-GUEST
access-group WIRELESS-CONTROL in interface WIRELESS-CONTROL
access-group WAAS in interface WAAS
access-group HIPAA in interface HIPAA
access-group WIRELESS-HIPAA-USERS in interface WIRELESS-HIPAA-USERS
access-group WIRELESS-HIPAA-DEVICES in interface WIRELESS-HIPAA-DEVICES
access-group MANAGEMENT_access_in in interface MANAGEMENT
access-group DROP-ALL in interface IPS-Mgmt
route MSP-WAN 0.0.0.0 0.0.0.0 10.10.255.11 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
aaa-server CiscoACS protocol tacacs+
aaa-server CiscoACS (MSP-WAN) host 192.168.42.131
 key *****
user-identity default-domain LOCAL
aaa authentication enable console CiscoACS LOCAL
aaa authentication http console CiscoACS LOCAL
aaa authentication ssh console CiscoACS LOCAL
aaa authorization command CiscoACS LOCAL
aaa accounting enable console CiscoACS
aaa accounting ssh console CiscoACS
aaa accounting command privilege 15 CiscoACS
aaa authentication secure-http-client
aaa local authentication attempts max-fail 6
aaa authorization exec authentication-server
http server enable
http server idle-timeout 15
http server session-timeout 15
http 192.168.41.101 255.255.255.255 MSP-WAN
http 192.168.41.102 255.255.255.255 MSP-WAN
http 192.168.42.122 255.255.255.255 MSP-WAN
http 192.168.42.124 255.255.255.255 MSP-WAN
http 192.168.42.133 255.255.255.255 MSP-WAN
http 192.168.42.138 255.255.255.255 MSP-WAN
http 192.168.42.139 255.255.255.255 MSP-WAN
http 192.168.42.134 255.255.255.255 MSP-WAN
snmp-server group V3Group v3 priv
```

```
snmp-server user ciscolms V3Group v3 encrypted auth sha
56:bd:0f:20:11:a7:78:6e:08:cc:a9:43:f7:86:0e:ab:04:7c:a7:db priv aes 256
56:bd:0f:20:11:a7:78:6e:08:cc:a9:43:f7:86:0e:ab:04:7c:a7:db:88:e3:53:03:7b:f1:02:30:bc:14:
98:e5
snmp-server user csmadmin V3Group v3 encrypted auth sha
56:bd:0f:20:11:a7:78:6e:08:cc:a9:43:f7:86:0e:ab:04:7c:a7:db priv aes 256
56:bd:0f:20:11:a7:78:6e:08:cc:a9:43:f7:86:0e:ab:04:7c:a7:db:88:e3:53:03:7b:f1:02:30:bc:14:
98:e5
snmp-server host MSP-WAN 192.168.42.134 version 3 ciscolms
snmp-server host MSP-WAN 192.168.42.139 version 3 ciscolms
snmp-server host MSP-WAN 192.168.42.133 version 3 csmadmin
snmp-server location Building SJC-17-1 Aisle 2 Rack 3
snmp-server contact Bart McGlothin
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
snmp-server enable traps syslog
snmp-server enable traps ipsec start stop
snmp-server enable traps memory-threshold
snmp-server enable traps interface-threshold
snmp-server enable traps remote-access session-threshold-exceeded
snmp-server enable traps connection-limit-reached
snmp-server enable traps cpu threshold rising
snmp-server enable traps ikev2 start stop
snmp-server enable traps nat packet-discard
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
ssh scopy enable
ssh 192.168.41.101 255.255.255.255 MSP-WAN
ssh 192.168.41.102 255.255.255.255 MSP-WAN
ssh 192.168.42.122 255.255.255.255 MSP-WAN
ssh 192.168.42.124 255.255.255.255 MSP-WAN
ssh 192.168.42.133 255.255.255.255 MSP-WAN
ssh 192.168.42.138 255.255.255.255 MSP-WAN
ssh 192.168.42.139 255.255.255.255 MSP-WAN
ssh 192.168.42.134 255.255.255.255 MSP-WAN
ssh timeout 15
ssh version 2
console timeout 15
dhcprelay server 192.168.42.130 MSP-WAN
dhcprelay enable POS
dhcprelay enable DATA
dhcprelay enable VOICE
dhcprelay enable WIRELESS
dhcprelay enable WIRELESS-POS
dhcprelay enable PARTNER
dhcprelay enable WIRELESS-GUEST
dhcprelay enable WIRELESS-CONTROL
dhcprelay enable HIPAA
dhcprelay enable WIRELESS-HIPAA-USERS
dhcprelay enable WIRELESS-HIPAA-DEVICES
dhcprelay timeout 60
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 192.168.62.162 source MSP-WAN
ntp server 192.168.62.161 source MSP-WAN prefer
ssl encryption aes128-sha1 aes256-sha1 3des-sha1
webvpn
 anyconnect-essentials
username csmadmin password <removed> encrypted privilege 15
username jchambers password <removed> encrypted privilege 15
username ciscolms password <removed> encrypted privilege 15
username bmcgloth password <removed> encrypted privilege 15
!
```

```
class-map inspection_default
 match default-inspection-traffic
class-map global-class-XXX
 match any
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 description IPS inspection policy for Cisco LAB
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
 class global-class-XXX
  ips inline fail-close
 class class-default
  ips promiscuous fail-open
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
password encryption aes
Cryptochecksum:0c17bedaf99e8d7c1ce43105b2a7d2c5
: end


IPS-A2-MSP-1# show configuration
! ------------------------------
! ------------------------------
! Version 7.1(6)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S648.0
! ------------------------------
service interface
exit
! ------------------------------
```

```
service authentication
attemptLimit 6
password-strength
size 7-64
digits-min 1
lowercase-min 1
other-min 1
number-old-passwords 4
exit
cli-inactivity-timeout 15
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 10.10.191.21/24,10.10.191.1
host-name IPS-A2-MSP-1
telnet-option disabled
access-list 192.168.41.101/32
access-list 192.168.41.102/32
access-list 192.168.42.122/32
access-list 192.168.42.124/32
access-list 192.168.42.133/32
access-list 192.168.42.134/32
access-list 192.168.42.138/32
access-list 192.168.42.139/32
login-banner-text WARNING: THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS
ONLY!
dns-primary-server enabled
address 192.168.42.130
exit
dns-secondary-server disabled
dns-tertiary-server disabled
exit
time-zone-settings
offset -480
standard-time-zone-name PST
exit
ntp-option enabled-ntp-unauthenticated
ntp-server 192.168.62.161
exit
summertime-option recurring
summertime-zone-name PDT
start-summertime
month march
week-of-month second
day-of-week sunday
time-of-day 02:00:00
exit
end-summertime
month november
week-of-month first
day-of-week sunday
time-of-day 02:00:00
exit
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
```

```
exit
! ------------------------------
service notification
trap-destinations 192.168.42.124
trap-community-name RSAenvision
exit
enable-notifications true
trap-community-name RSAenvision
system-location Building SJC-17-1 Row 1 Rack 1
system-contact EmployeeA
exit
! ------------------------------
service signature-definition sig0
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
enable-tls true
port 443
server-id IPS-A2-MSP-1
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
! ------------------------------
service global-correlation
exit
! ------------------------------
service aaa
aaa radius
primary-server
server-address 192.168.42.131
shared-secret <removed>
exit
nas-id IPS-A2-MSP-1
local-fallback enabled
console-authentication radius-and-local
default-user-role administrator
exit
exit
! ------------------------------
service analysis-engine
virtual-sensor vs0
physical-interface PortChannel0/0
exit
exit
IPS-A2-MSP-1#
```

S-A2-MSP-1

```
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname S-A2-MSP-1
!
logging buffered 50000 debugging
enable secret 5 <removed>
!
username bart privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
!
aaa new-model
aaa authentication login CiscoACS group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
system mtu routing 1500
ip subnet-zero
no ip source-route
ip domain-name cisco-irn.com
ip name-server 192.168.42.130
!
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh version 2
ip scp server enable
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
!
password encryption aes
!
crypto pki trustpoint TP-self-signed-4189032704
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-4189032704
 revocation-check none
 rsakeypair TP-self-signed-4189032704
!
!
crypto pki certificate chain TP-self-signed-4189032704
 certificate self-signed 01
  <removed>
  quit
!
!
archive
```

```
 log config
  logging enable
  hidekeys
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0
 no ip address
 shutdown
!
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/2
 description AIR-CAP3502I
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 18
 switchport trunk allowed vlan 14-18
 switchport mode trunk
!
interface GigabitEthernet0/3
!
interface GigabitEthernet0/4
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/5
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/6
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/7
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/8
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/9
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/10
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/11
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/12
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/13
 switchport access vlan 17
```

```
 shutdown
!
interface GigabitEthernet0/14
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/15
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/16
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/17
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/18
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/19
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/20
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/21
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/22
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/23
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/24
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/25
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/26
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/27
 switchport access vlan 17
 shutdown
!
interface GigabitEthernet0/28
 switchport access vlan 17
 shutdown
!
interface TenGigabitEthernet0/1
 shutdown
```

```
!
interface TenGigabitEthernet0/2
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan1000
 description Management VLAN for Switch
 ip address 10.10.191.11 255.255.255.0
!
ip default-gateway 10.10.191.1
ip classless
no ip forward-protocol nd
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication CiscoACS
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Vlan1000
!
!
logging trap debugging
logging source-interface Vlan1000
logging 192.168.42.124
access-list 23 permit 192.168.41.101 log
access-list 23 permit 192.168.41.102 log
access-list 23 permit 192.168.42.111 log
access-list 23 permit 192.168.42.122 log
access-list 23 permit 192.168.42.124 log
access-list 23 permit 127.0.0.1 log
access-list 23 permit 192.168.42.131 log
access-list 23 permit 192.168.42.133 log
access-list 23 permit 192.168.42.138 log
access-list 23 permit 10.19.151.99 log
access-list 23 deny   any log
access-list 88 permit 192.168.42.124 log
access-list 88 deny   any log
snmp-server engineID remote 192.168.42.124 0000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access 88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
snmp-server trap-source Vlan1000
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps power-ethernet group 1
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
```

```
snmp-server enable traps vlan-membership
snmp-server host 192.168.42.124 remoteuser
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 <removed>
radius-server source-ports 1645-1646
!
control-plane
!
banner exec ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                  **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO ****
                  **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
 session-timeout 15  output
 exec-timeout 15 0
 login authentication CiscoACS
line vty 0 4
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication CiscoACS
 transport preferred none
```

```
 transport input ssh
 transport output none
!
ntp clock-period 36026372
ntp source Vlan1000
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end
```