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."

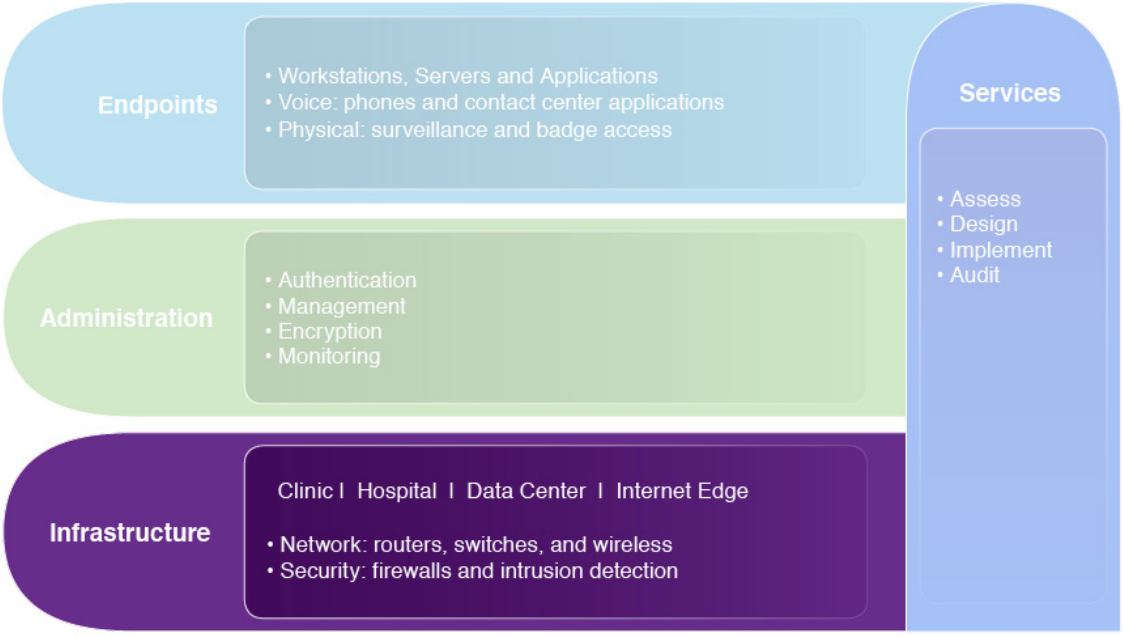
Although every company has specific considerations that vary from this implementation, these designs and the configurations of the components in Appendix E, "Detailed Full Running Configurations," provide an instructive example of what is needed to secure PHI. Each component selected was assessed for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

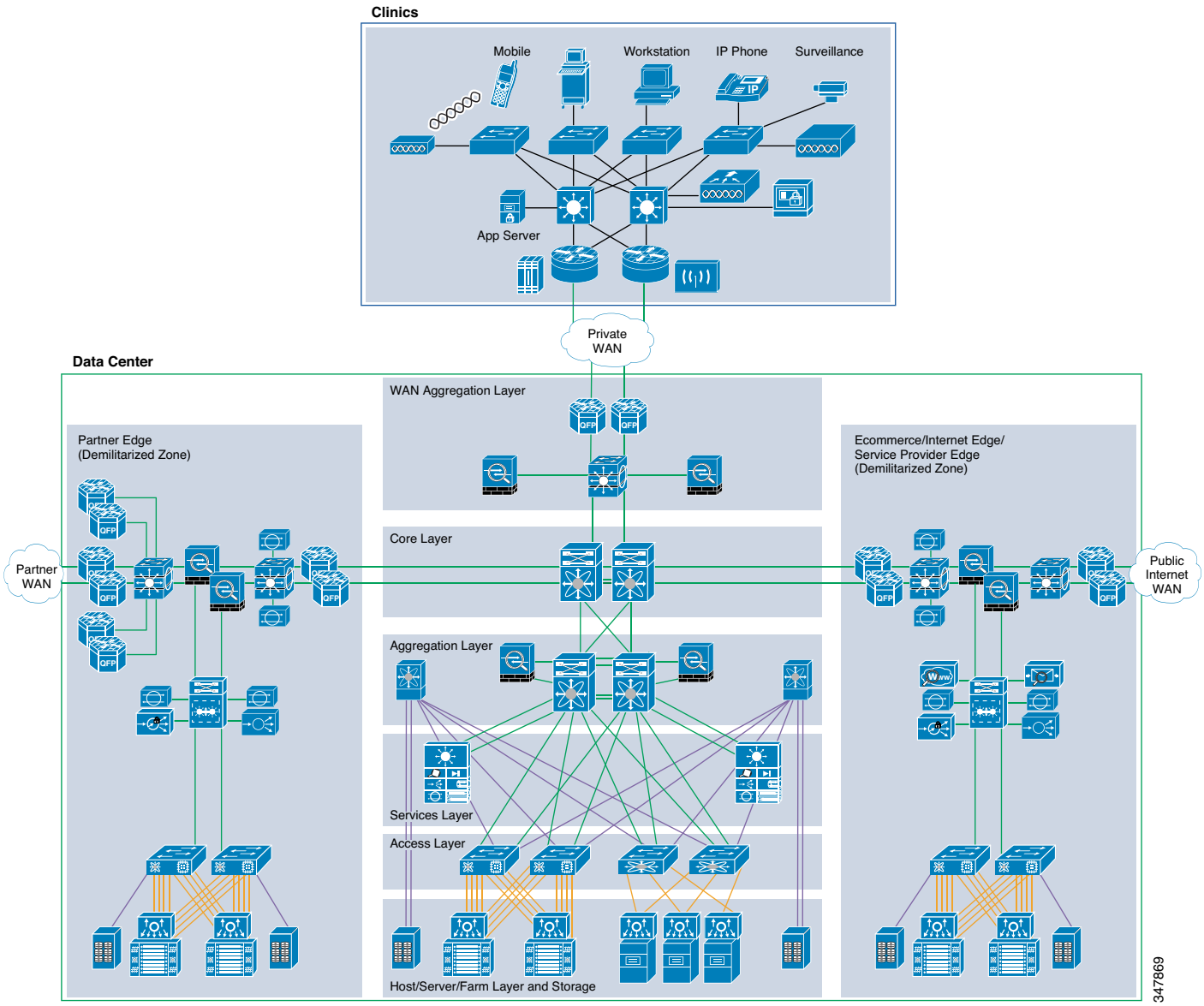
***Figure 4-1 Infrastructure Layer of the Solution Framework***




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

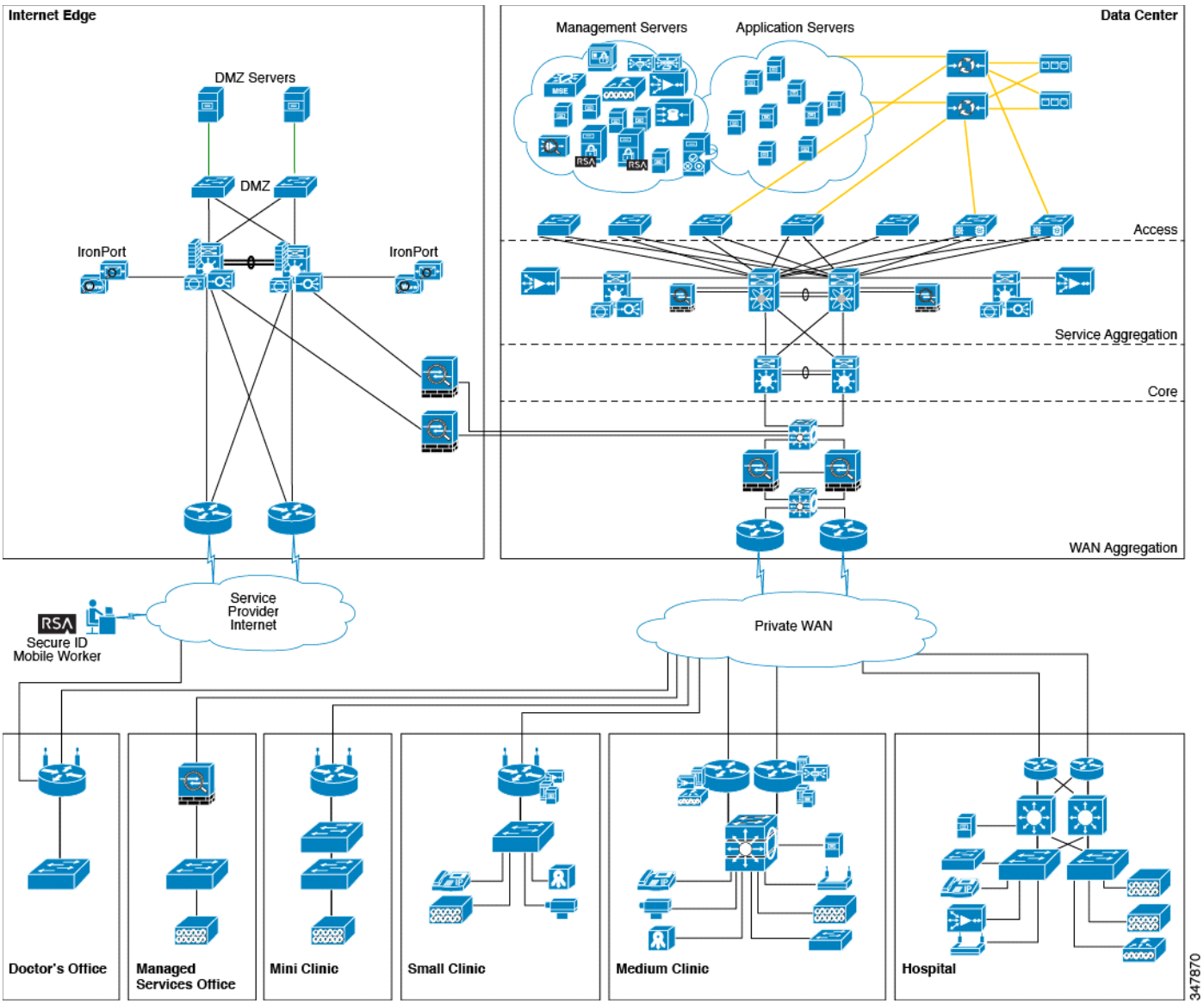
Figure 4-2 shows the enterprise-wide reference architecture.

***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."

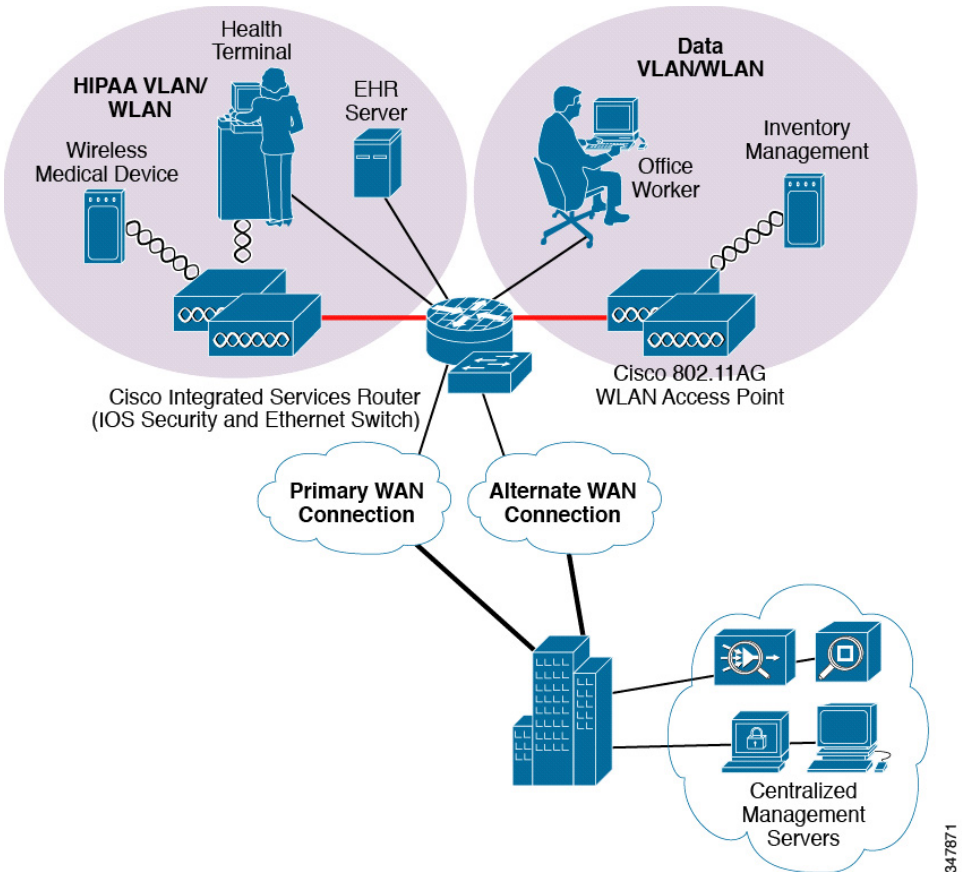
**Note** Each of these designs includes a variety of components that can be interchangeably used between them, depending on business requirements. For validation purposes, it was not necessary to implement all possible components in each design.

## 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:

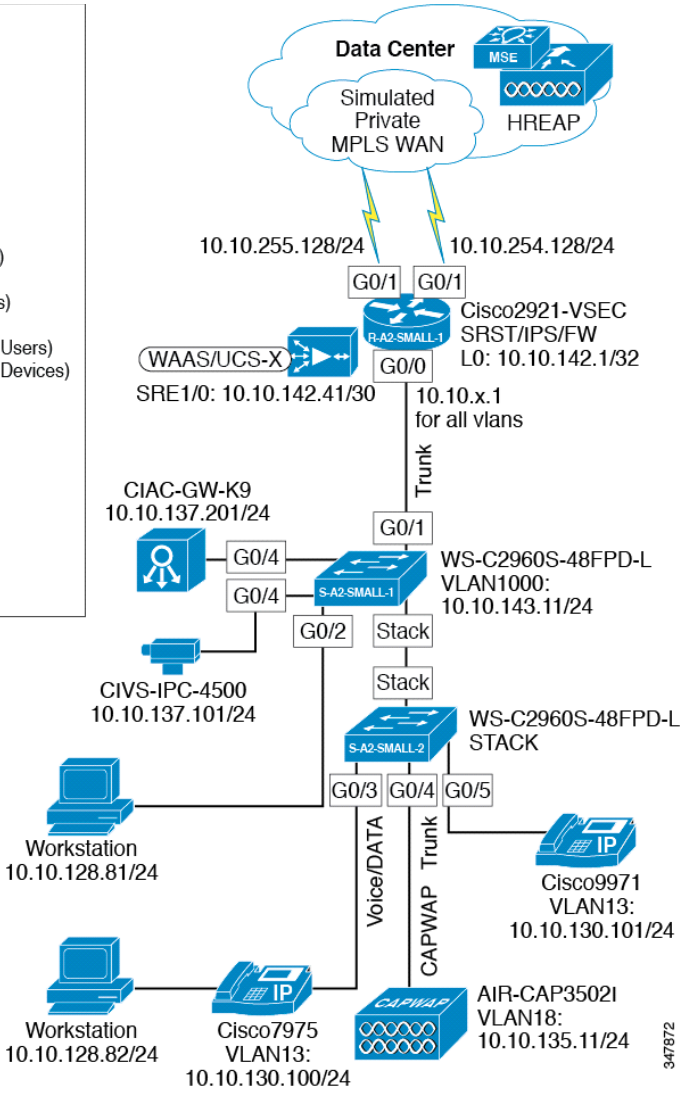
- Compromises in network resilience commensurate with the priority of treatment
- Some potential downtime because of single points of failure, demanding local replacement support

# 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

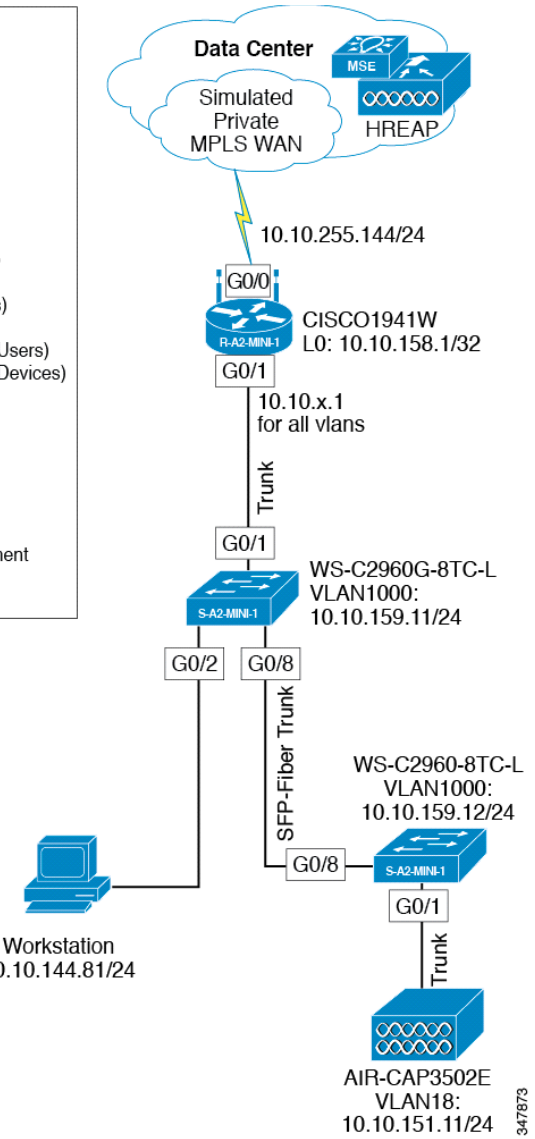
- Cisco 2921 Integrated Services Router (ISR)
- Cisco Catalyst 2960S 48-port PoE switch
- Cisco Aironet 3502i Access Points
- Cisco Video Surveillance 4500 Series IP Cameras
- Cisco Physical Access Gateway

## 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 | |



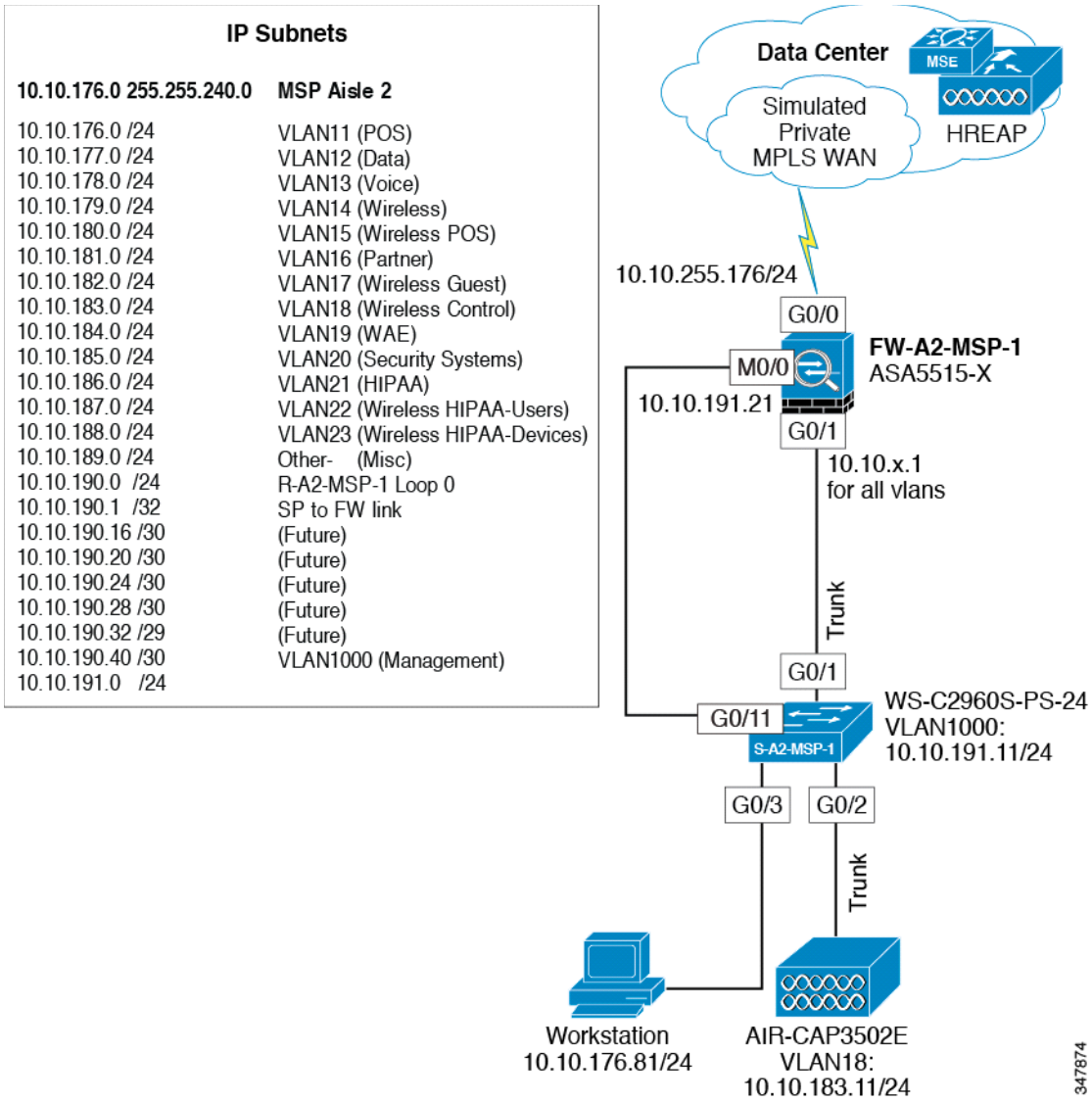

### Components Selected

- 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

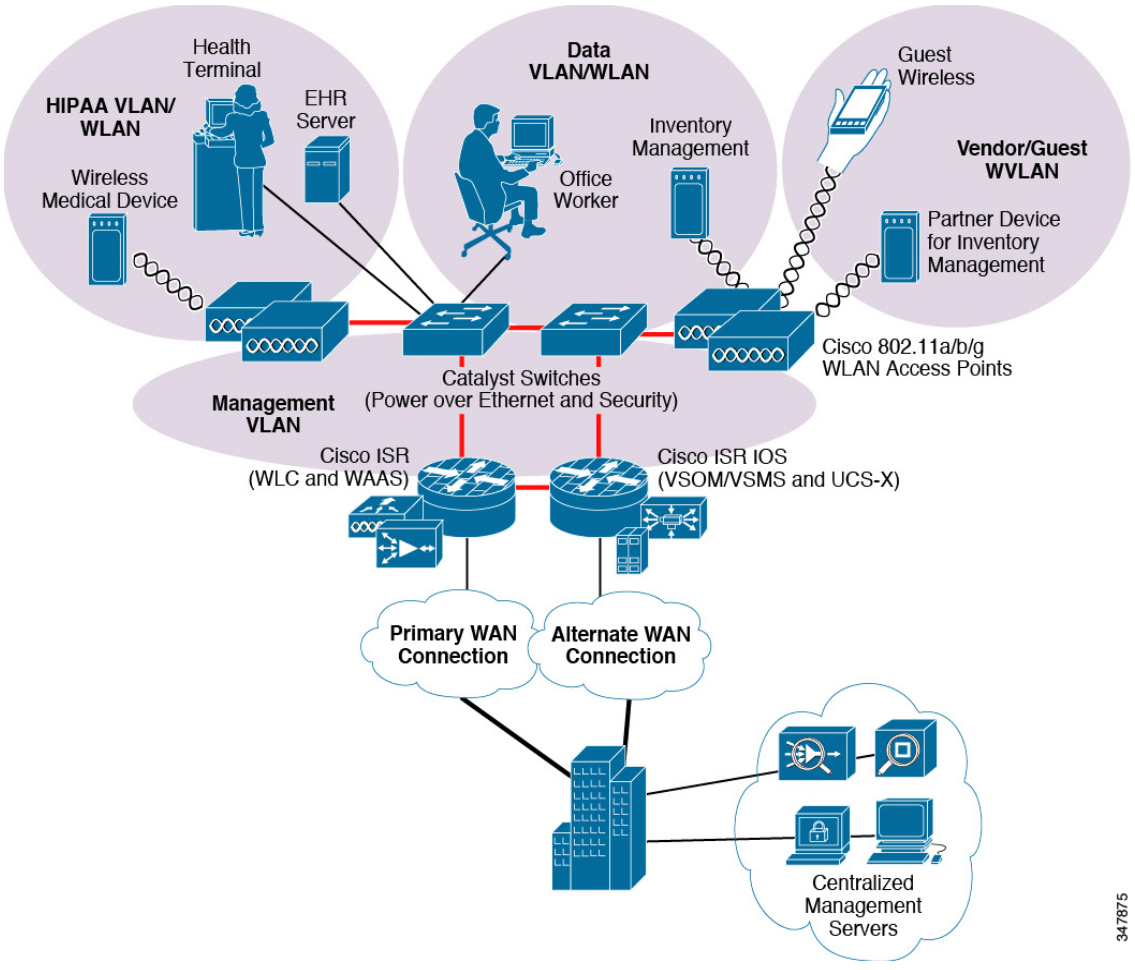
- Cisco ASA 5515-x Firewall with vIPS
- Cisco Catalyst 2960S Switch
- Cisco Aironet 3502e Access Points

## 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

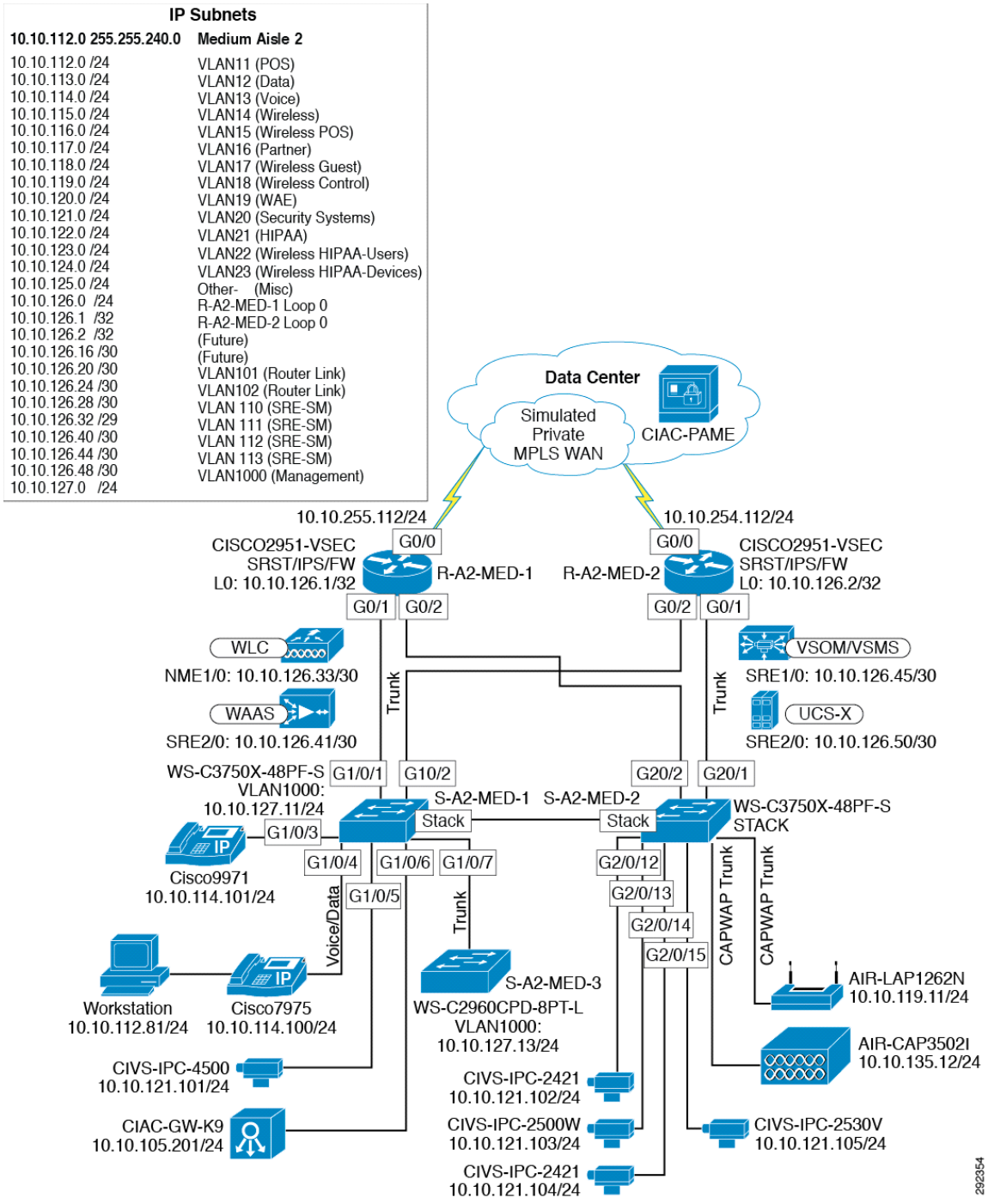
Limitations include the following:

- 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

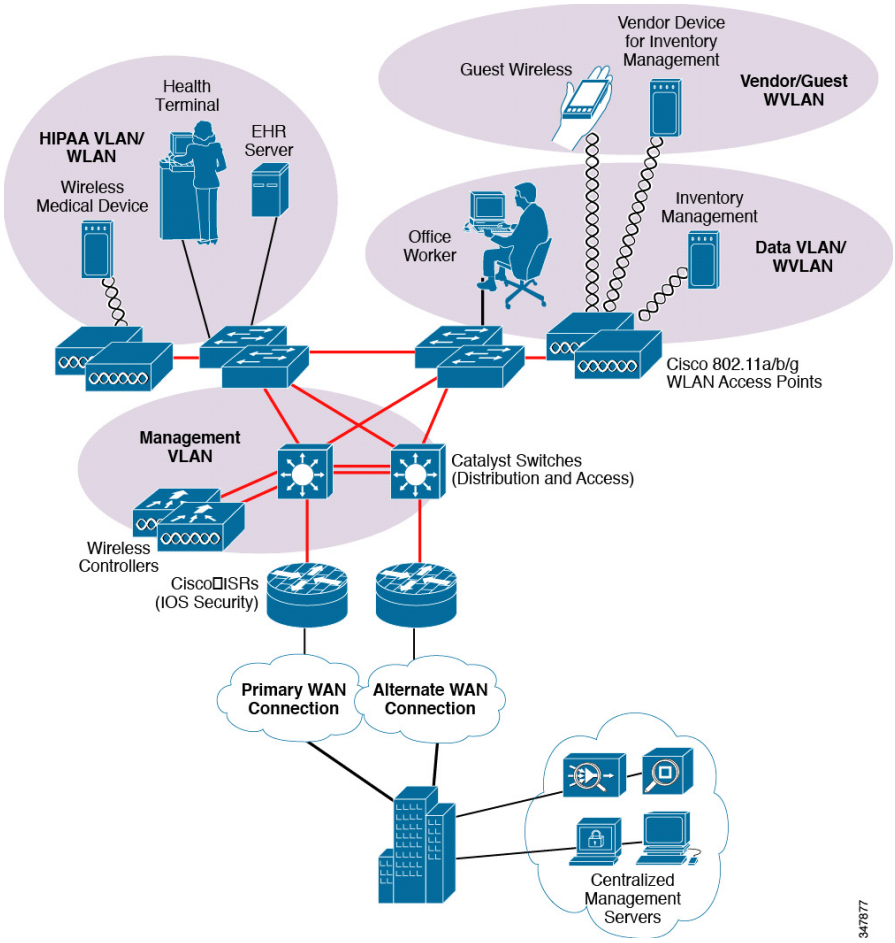
- Cisco 2951 Integrated Services Router (ISR)
- Cisco Catalyst 3750X 48-port PoE Switch
- Cisco Catalyst 2960 Compact Switch
- Cisco Aironet 3502e and 1262N Access Points
- Cisco Video Surveillance 2421 IP Dome Camera
- Cisco Video Surveillance 2500 Series IP Camera
- Cisco Operations Manager v4.1
-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

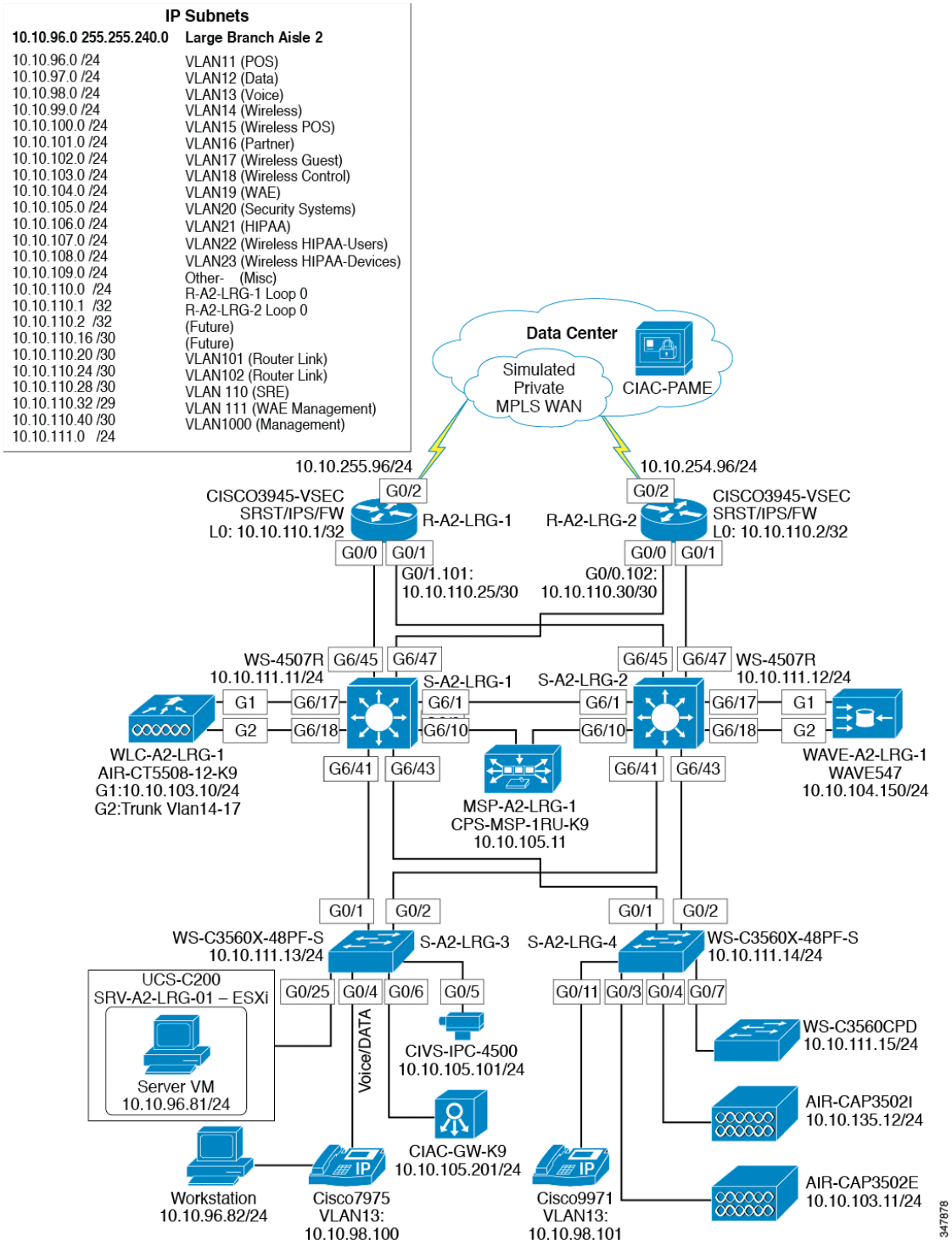
Limitations include the following:

- 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***



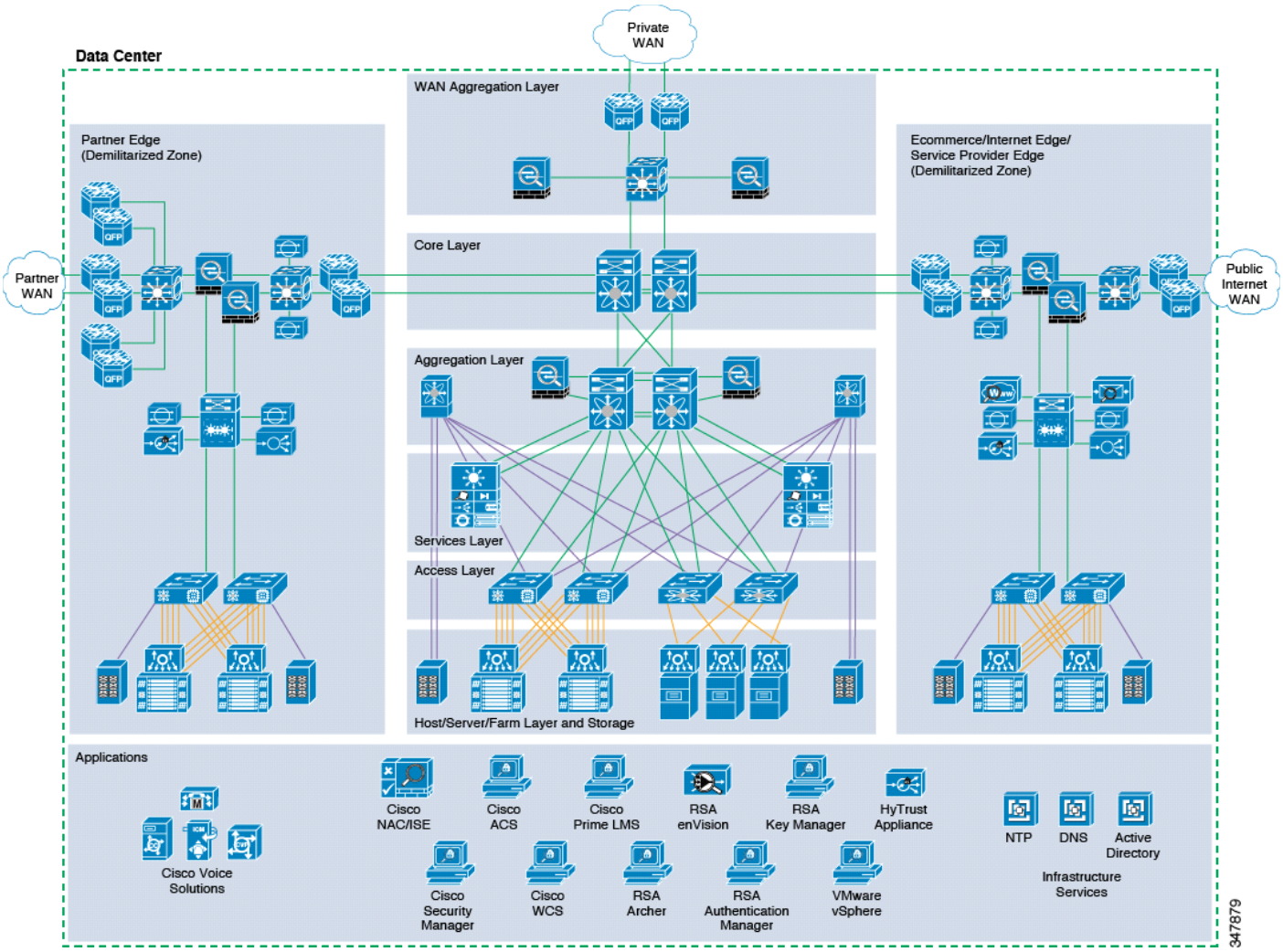
### Components Selected

- 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***



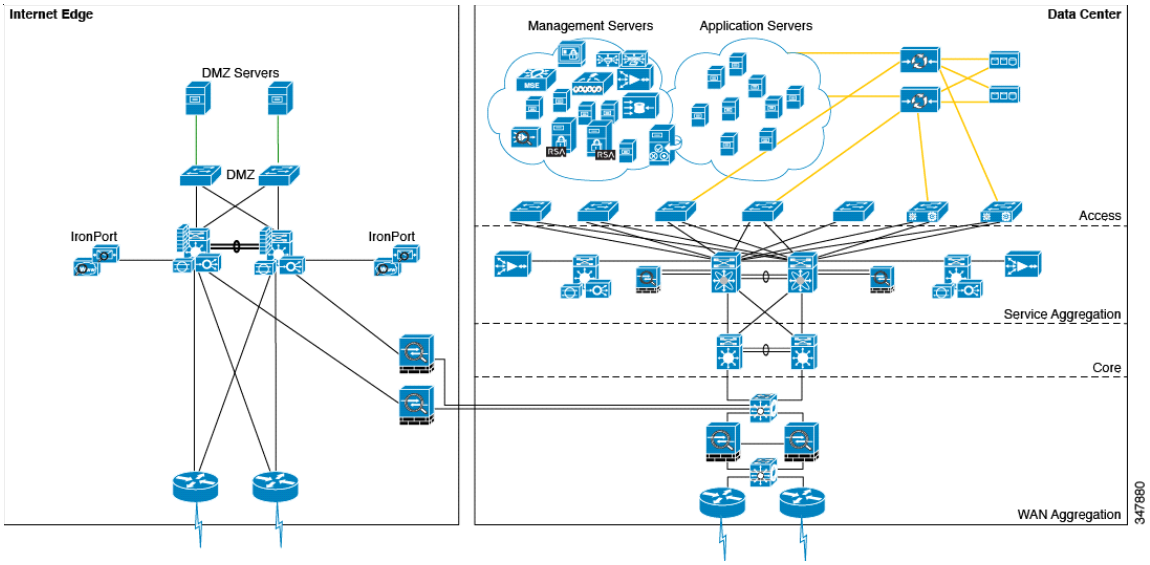

Design considerations are as follows:

- 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***



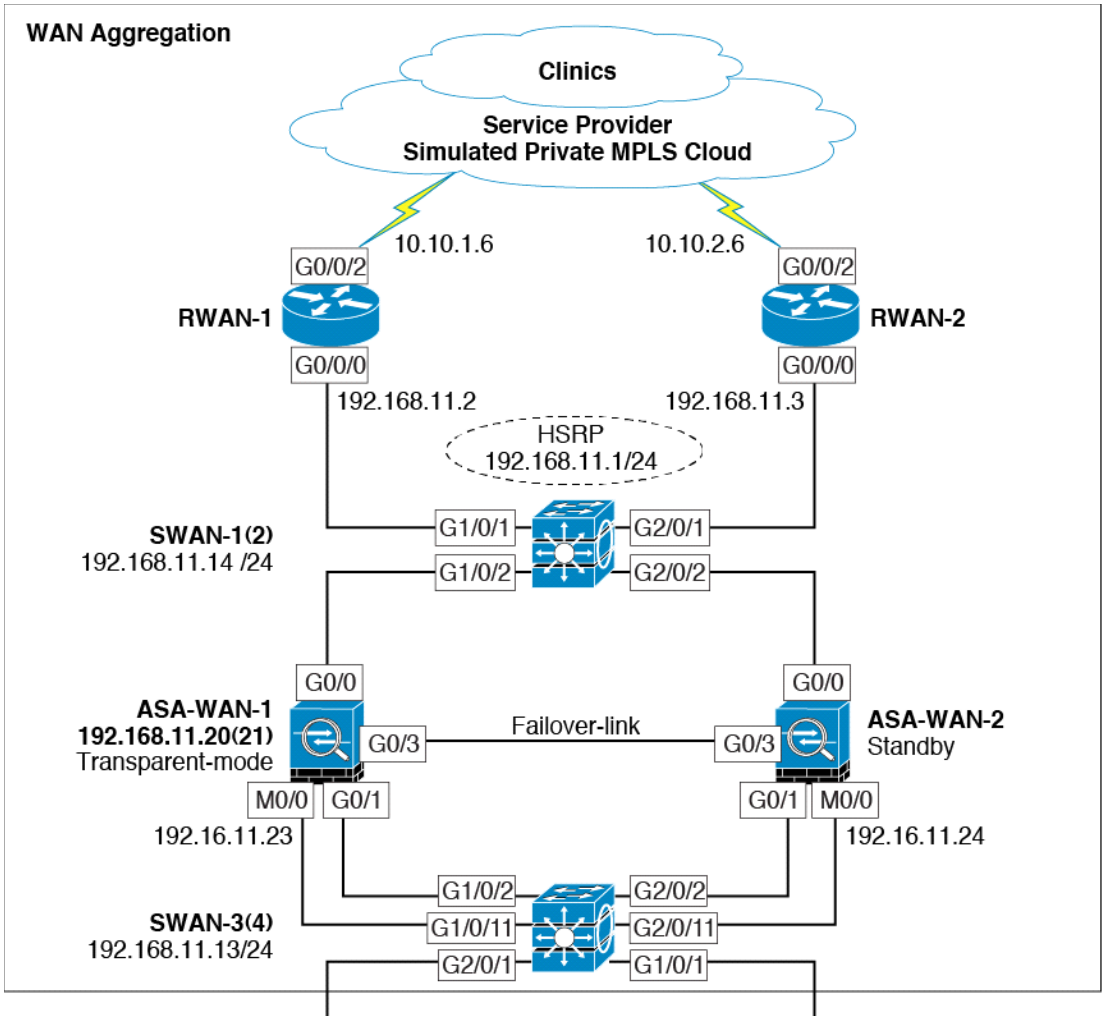

Data centers can house many types of functions, and the term itself can encompass narrow and broad aspects. For the purposes of this guide, data centers include the following functions:

- 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*



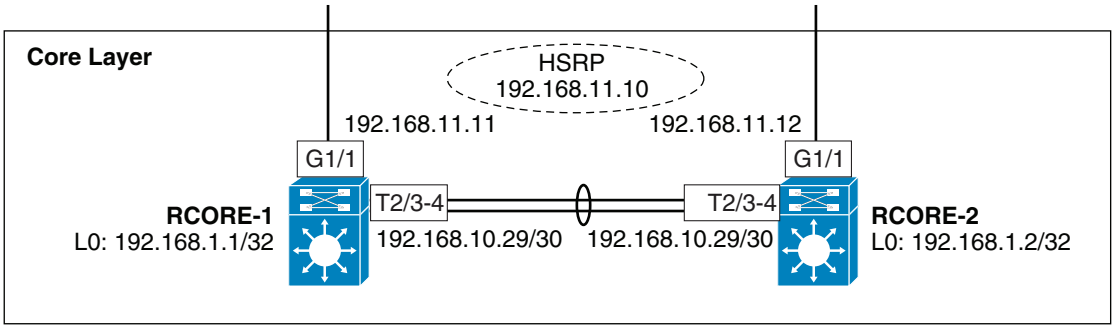

## Components Selected

- 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

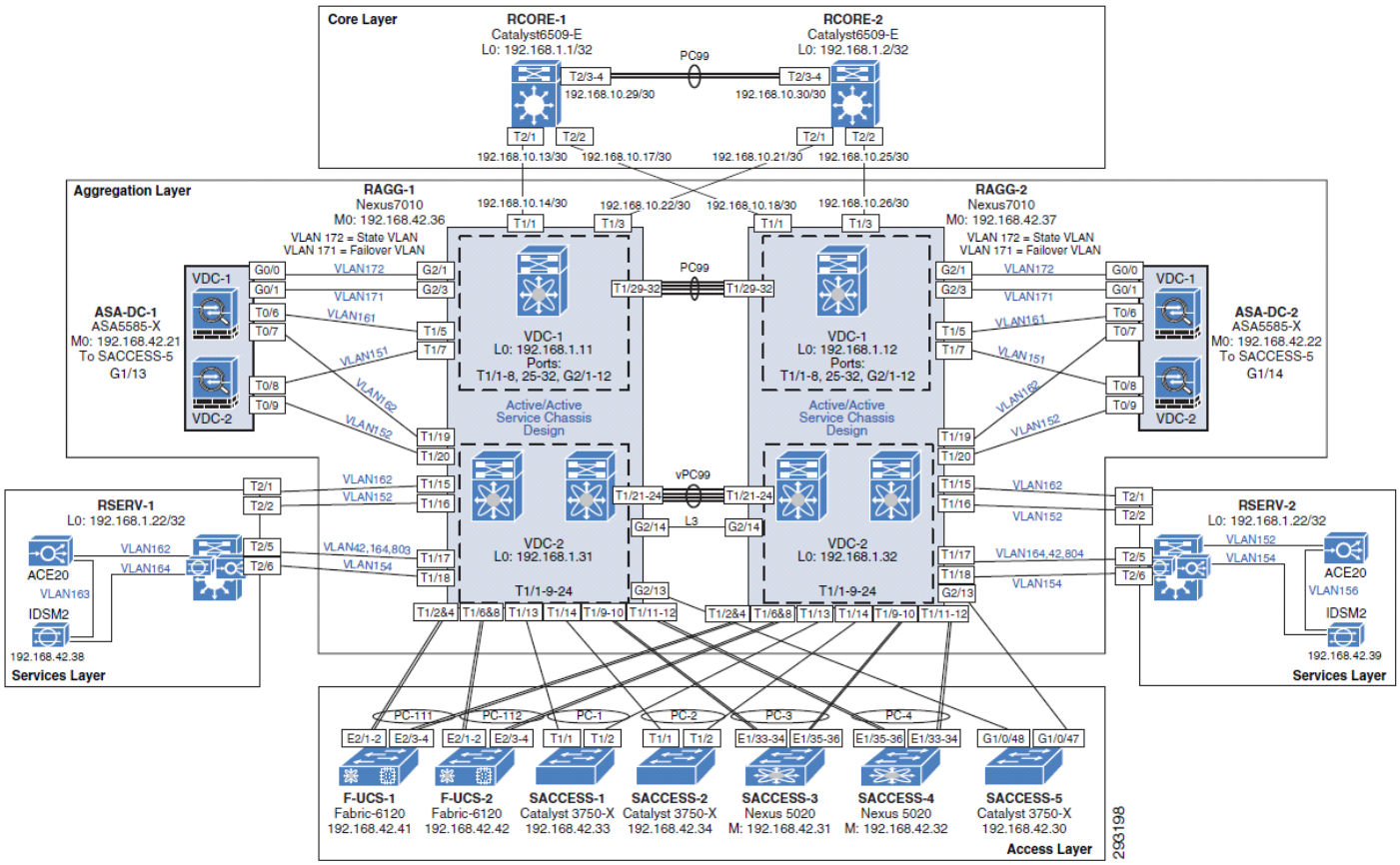
- Cisco Catalyst 6500-E Switch

**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***



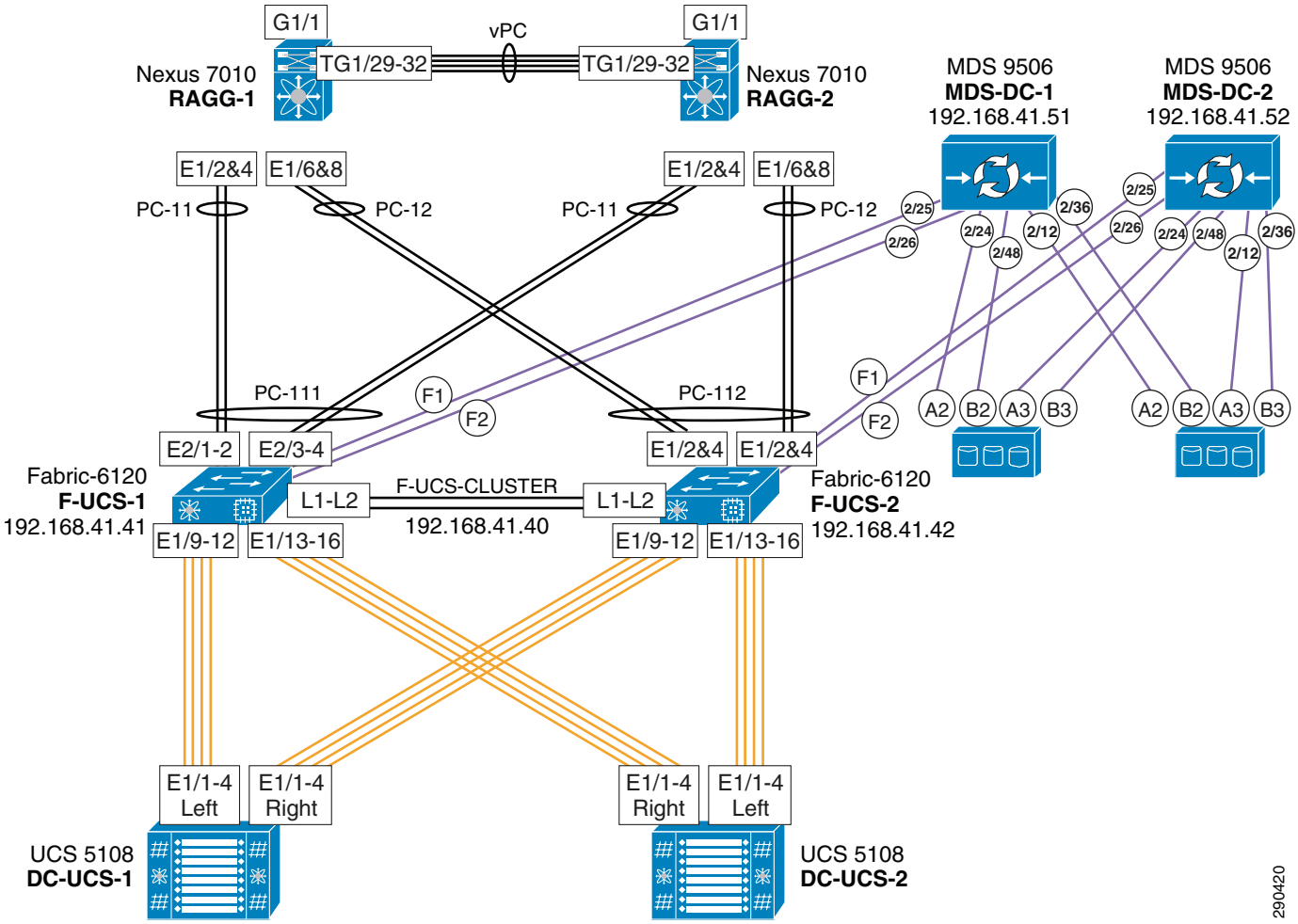

## Components Selected

- 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***



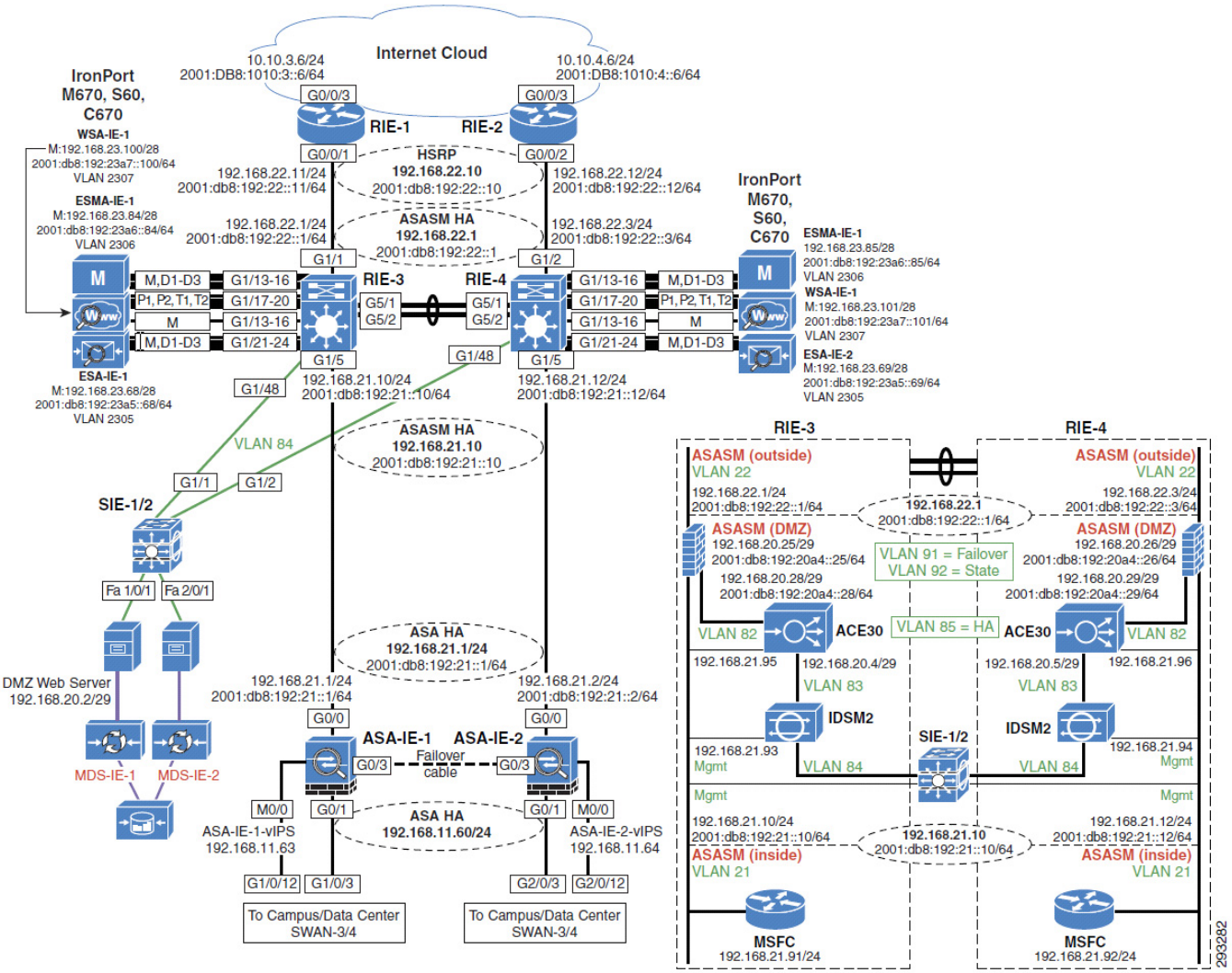

## Components Selected

- 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***



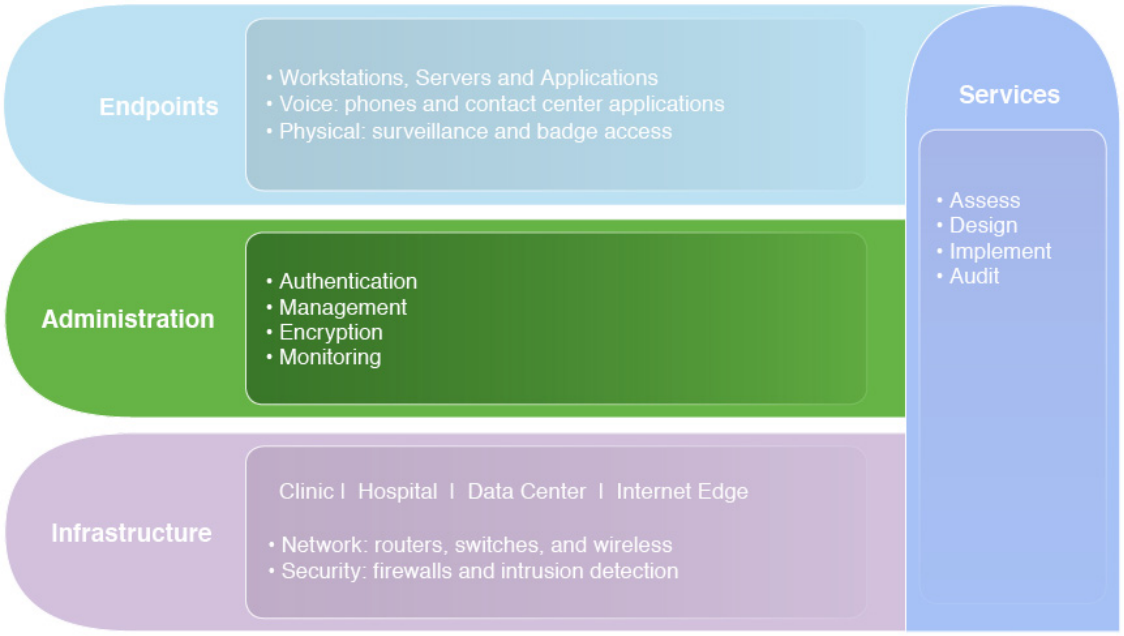

## Components Selected

- 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

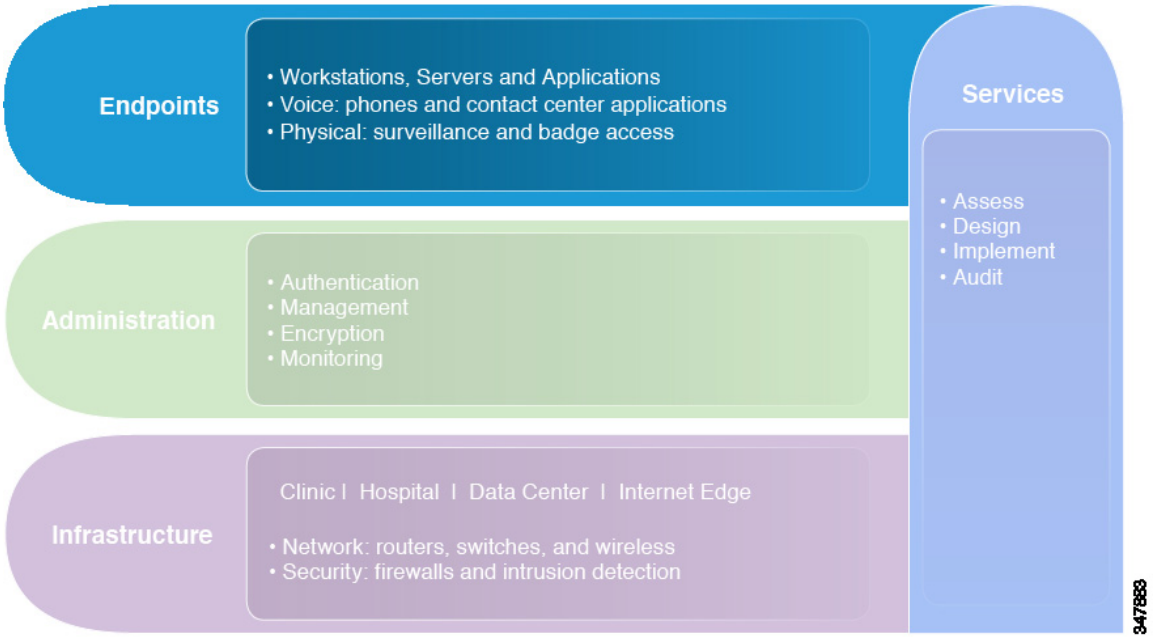
## Components Selected

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

*Table 4-1 HIPAA Safeguards Supported (continued)*

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

*Table 4-1 HIPAA Safeguards Supported (continued)*

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

*Table 4-1 HIPAA Safeguards Supported (continued)*

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

*Table 4-1 HIPAA Safeguards Supported (continued)*

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

*Table 4-1 HIPAA Safeguards Supported (continued)*

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

*Table 4-1 HIPAA Safeguards Supported (continued)*

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

*Table 4-1 HIPAA Safeguards Supported (continued)*

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