



Newer Cisco SBA for Government Guides Available

This guide is part of an older series of Cisco Smart Business Architecture for Government. To access the latest Cisco SBA for Government Guides, go to <http://www.cisco.com/go/govsba>

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.





SBA
FOR
GOVT

LARGE

BORDERLESS
NETWORKS

Internet Edge Deployment Guide

● ● ● SBA FOR GOVERNMENT

Using this Borderless Networks Guide

This document is for the reader who:

- Has 2000–10,000 connected employees
- Wants more secure access to the Internet
- Wants to provide backup connectivity to the Internet for employees
- Requires a solution for teleworker and mobile worker access to the agency's data
- Requires a solution to control employee access to the Internet and block malicious websites
- Requires a solution to filter SPAM and malicious email sent to the agency
- Requires a solution to improve the availability of Internet-facing services
- Has IT workers with a CCNA® certification or equivalent experience
- Wants to deploy their network infrastructure efficiently
- Wants the assurance of a tested solution
- Requires a migration path for growth

Notes

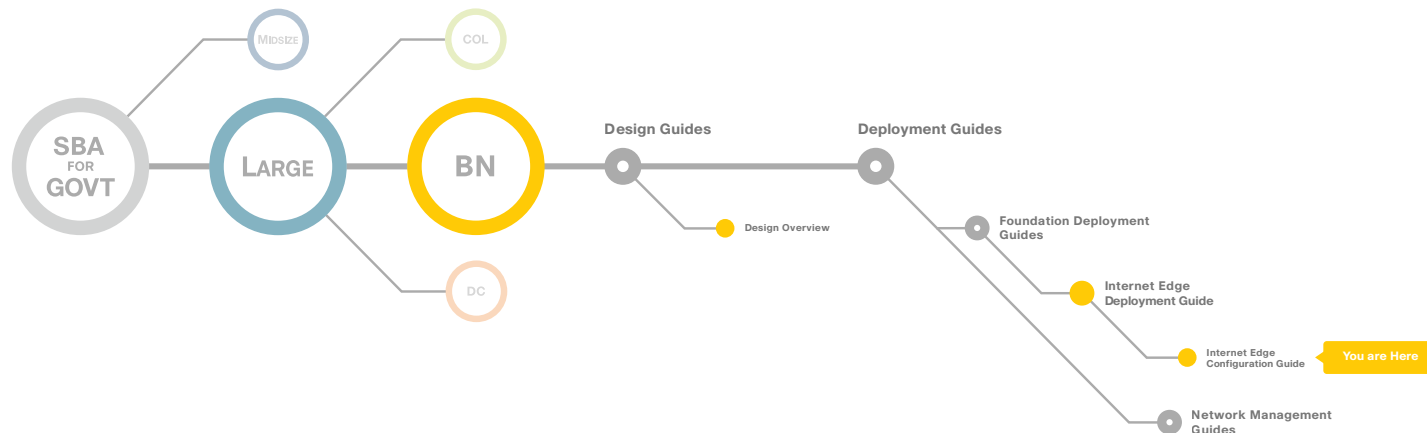


Table of Contents

Introduction	1	Email Security	65
Internet Edge Agency Overview	5	Web Security	78
Architecture Overview: Internet Edge.....	6	Internet Edge Server Load Balancing	100
Internet Edge Connectivity.....	8	Summary	105
Firewall	11	Appendix A: Large Agencies Deployment Product List.....	106
Intrusion Prevention.....	38	Appendix B: SBA for Large Agencies Document System.....	108
Remote Access VPN.....	49		

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental. Cisco Unified Communications SRND (Based on Cisco Unified Communications Manager 7.x)

© 2010 Cisco Systems, Inc. All rights reserved.

Introduction

The Cisco Smart Business Architecture (SBA) for Government Large Agencies—Borderless Networks is designed for networks that have 2000 to 10,000 connected users. We created a prescriptive, out-of-the-box deployment guide that is based on best-practice design principles and that delivers flexibility and scalability. The deployment guides are designed to make the Borderless Network for Large Agencies easy—easy to configure, easy to deploy, and easy to manage.

The goal of any network implementation is to support the applications that benefit the users and the agency that it is built for. As they guide you through the depth and breadth of the architecture, the SBA deployment guides are intended to simplify navigating among and learning the various networking technologies that we used to build the architecture. The SBA is a solid network foundation that provides the flexibility to support new user or network services without re-engineering the network.

Using the Deployment Guides

The SBA for Large Agencies architecture was designed, built, and validated as an end-to-end system.

To focus on specific elements of the architecture, there are three primary deployment guides, one each for local-area network (LAN), wide-area network (WAN), and Internet Edge. To enhance the SBA for Large Agencies architecture, there are a number of supplemental guides that address specific functions, technologies, or features that may be important to solving your operational problems. Within each of these deployment guides, you will find a modular approach that allows you to start at the beginning and work your way through or to jump to a specific module. Each deployment guide and the modules within are designed to stand alone, so that you can deploy the specific Cisco technology in a module without completing each previous module. Each deployment guide includes a complete list of the products and the software revisions tested, and a companion supplemental guide contains all configuration files used.

The deployment guides begin with an agency overview of the common operational problems addressed, followed by an architecture overview to assist you with matching the value of a technology solution to your operational problems.

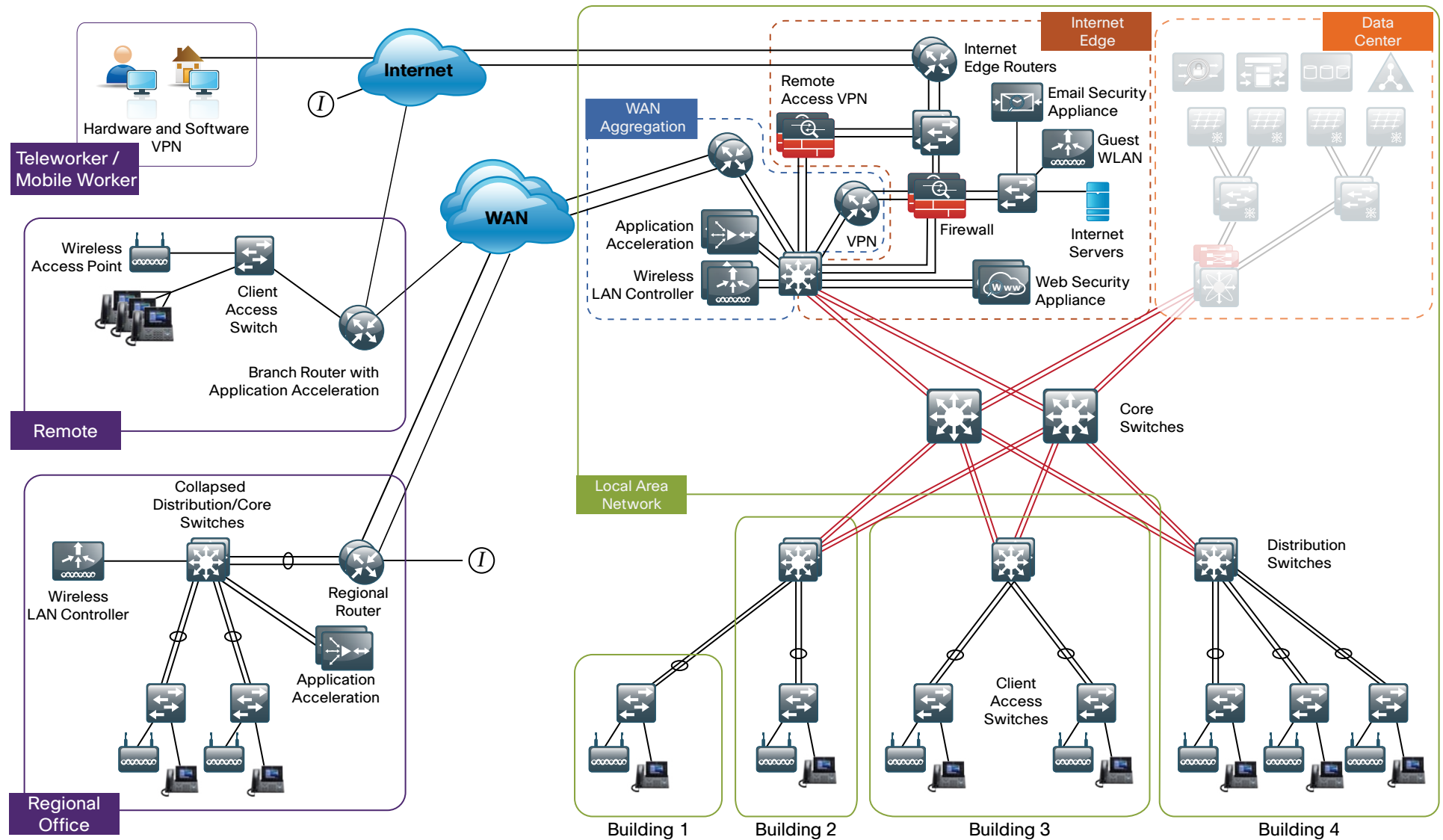
The **LAN Deployment Guide** covers wired and wireless network access with ubiquitous capabilities for both the larger campus-size LAN as well as the smaller remote site LAN. Resiliency, security, and scalability are included to provide a robust communications environment. Quality of service (QoS) is integrated to ensure that the base architecture can support a multitude of applications including low-latency, drop-sensitive multimedia applications coexisting with data applications on a single network. The guide also provides a guest and partner access solution that is secured from accessing internal confidential information while using the same wireless infrastructure that employees use.

The **WAN Deployment Guide** includes the primary site aggregation design as well as multiple remote site designs to accommodate varying scale and service-level requirements in a common approach. The flexibility in the WAN deployment guide provides guidance and configuration for Multiprotocol Label Switching (MPLS) transport as well as broadband or Internet transport in a primary or backup role. QoS is integrated to ensure that the base architecture can support a multitude of applications on a single transport. The design integrates application optimization and the deployment guide provides details on optimizing WAN traffic to ensure economical use of bandwidth while providing a good user experience.

The **Internet Edge Deployment Guide** focuses on security services such as firewalls and intrusion prevention systems to protect your agency's gateway to the Internet. Internet service provider connectivity and routing options, combined with server load balancing, provide resiliency to the design. The Email Security module covers protecting email from spam and malware. The Web Security module provides acceptable-use control and monitoring as well as managing the increasing risk associated with clients browsing the Internet. The VPN design supports the teleworker and mobile user with secure remote access. All of these elements are covered in separate modules and yet are designed to work together to provide a secure Internet Edge solution.

Figure 1 shows the components of the SBA for Large Agencies—Borderless Networks.

Figure 1. SBA for Large Agencies—Borderless Networks Overview



Design Goals

This architecture is based on requirements gathered from customers, partners, and Cisco field personnel for agencies with 2000 to 10,000 connected users. When designing the architecture, we considered the gathered requirements and the following design goals:

- **Ease of Deployment:** Agencies can deploy the design consistently across all products included in the architecture. The configurations used in the deployment represent a best-practice methodology to enable a fast and resilient deployment.
- **Flexibility and Scalability:** The architecture can grow with the agency without being redesigned.
- **Resiliency and Security:** The architecture keeps the network operating even during unplanned outages and attacks.
- **Easy to Manage:** The deployment guidance includes configuring devices to be managed by a network management system (NMS) or as unique elements of the network.
- **Advanced Technology Ready:** Implementing advanced technologies like collaboration is easy because the network foundation is already configured with the required baseline network services.

Ease of Deployment, Flexibility and Scalability

Agencies of 2000 to 10,000 users are often spread out among different geographical locations. The locations might have labels like remote site, regional site, or headquarters. This architecture addresses how to build a network for all these locations, irrespective of the label.

In this design, several methods are used to create and maintain a scalable network. Defining a common framework with a convergence of design standards drives global consistency and optimizes the design process, which ultimately results in lower cost and complexity. Standardization is the key to scalability; by keeping a small number of standard designs for common portions of the network, support staff are able to design services for, implement, and support these network areas more effectively.

To enhance scalability, we take a modular design approach; beginning with a set of standard, global building blocks, we can assemble a scalable network to meet requirements. For instance, to build a campus network, we might start with a LAN module, connect an Internet edge module, and then add a WAN module.

Many of these plug-in modules look identical for several different service areas; this provides consistency and scalability in that the same support methods can be used in multiple areas of the network to maintain the network. These modules follow standard core-distribution-access network design models and use layer separation to ensure that interfaces between the plug-ins are well defined.

Resiliency and Security

One of the keys to maintaining a highly available network is building the appropriate redundancy to guard against failure in the network, whether it is link, port, card, or chassis failure. But systems can be engineered to be too redundant, exhibiting failures of overly complex redundancy features, which results in complete communications failure. The redundancy in our architecture is carefully balanced with the complexity inherent in redundant systems.

Building production network services without any form of redundancy is unacceptable to most agencies. When building in the necessary redundancy, care must also be taken to prevent large dependency chains that result in greater risk of system failure. For example, chains of devices that do not have multiple cross-connections may create a dependency on both chains being completely available.

With the addition of a significant amount of delay-sensitive and drop-sensitive traffic such as voice and video conferencing, we also place a strong emphasis on recovery times. Choosing designs that reduce the time between failure detection and recovery is important for ensuring that the network stays available even in the face of a minor component failure.

Security of the network is also a very strong component of the architecture. In a large network, there are many entry points and we ensure that they are as secure as possible without making the network too difficult to use. Securing the network not only helps keep the network safe from attacks but is also a key component to network-wide resiliency.

Easy to Manage

While this guide focuses on the deployment of the network foundation, the next phase management and operation are considered. The configurations in the deployment guides are designed to allow the devices to be managed both via normal device management connections, such as SSH and HTTPS, but also via NMS. The configuration of the NMS is not covered in this guide.

Advanced Technology Ready

Flexibility, scalability, resiliency, and security all are characteristics of an advanced technology-ready network. The modular design of the architecture means that technologies can be added when the agency is ready to deploy them. However, the deployment of advanced technologies, such as collaboration, is eased because the architecture includes products and configurations that are ready to support collaboration from day one. For example, access switches provide Power over Ethernet (PoE) for phone deployments without the need for a local power outlet. The entire network is preconfigured with QoS to support high-quality voice. Multicast is configured in the network to support efficient voice and broadcast-video delivery.

Beyond the wired network, the wireless network is also preconfigured for devices that send voice over the wireless LAN, providing IP telephony over 802.11 Wi-Fi (referred to as mobility) at all locations. The Internet edge is also ready to provide soft phones via VPN, as well as traditional hard or desk phones.

Notes

Internet Edge Agency Overview

The Internet Edge addresses the following operational problems:

- Government agencies need to provide users access to Internet services (email and web)
- Users need access to services inside the agency from remote locations
- Agencies need to provide controlled access to data and/or services for the public, partners, and customers
- Agencies need to improve employee productivity by controlling Internet web access to work-related locations
- Agencies need to manage security risk associated with Internet connectivity

The Internet Edge provides connectivity for traffic traversing between the agency and the Internet. This includes traffic to and from the agency, the Internet, and DMZs. An agency's Internet Edge deployment needs to enforce the agency security policy and function as a real-world representation of that policy.

The services that the Internet Edge provides are connectivity to the Internet Service Provider, resiliency for Internet services, and access control for services like email, instant messaging, and web. As part of this access, appropriate use of Internet services by employees is an important consideration, as it helps to maintain productivity, avoid legal issues, and reduce costs associated with non-work-related bandwidth consumption.

Another service provided by the Internet Edge is access for a user from anywhere and allowing them access to the services and data they require to perform their role. In the Borderless Networks being deployed today, a user could be an employee, a contractor, a partner, or a customer. Each user has different needs for access, data, and the services that should be available.

As users' Internet access requirements broaden, the risk associated with such access has to be managed. There are three main types of risk that need to be managed; attacks against services, attacks against clients, and attacks that involve tricking a user into clicking on a malicious website or opening up a file that contains malicious code. The result of not protecting the agency against this activity includes loss of intellectual property, data theft, or even potential legal liability.

Architecture Overview: Internet Edge

This architecture uses a modular design model that breaks the Internet Edge up into functional blocks by service. By modularizing the design an agency can deploy the services as required.

The Internet Edge design includes the following modules:

1. **Internet Routing:** provides connectivity to one or more Internet Service Providers (ISP)
2. **Firewall:** Control access into and out of the different segments of the Internet Edge and provide a suite of other services like NAT
3. **Intrusion Prevention:** inspection of traffic traversing the Internet Edge looking for malicious behaviors
4. **Remote Access VPN:** Remote access functionality inside the firewall provides secure, consistent access to resources regardless of where the user is when connecting
5. **Email Security:** provides SPAM and malware filtering service to manage the risk associated with email
6. **Web Security:** provides acceptable use control and monitoring while at the same time managing the increasing risk associated with clients browsing the Internet
7. **Internet Edge Server Load Balancing:** load balances web services to the public and private network

The requirements for each agency will differ based on many factors, however the size of an agency's workforce is a good general starting point, and therefore, two designs based on user count are provided. The two Internet Edge designs are referred to as Internet Edge 5K and Internet Edge 10K.

Figure 2. Internet Edge in the SBA for Large Agencies—Borderless Networks Design

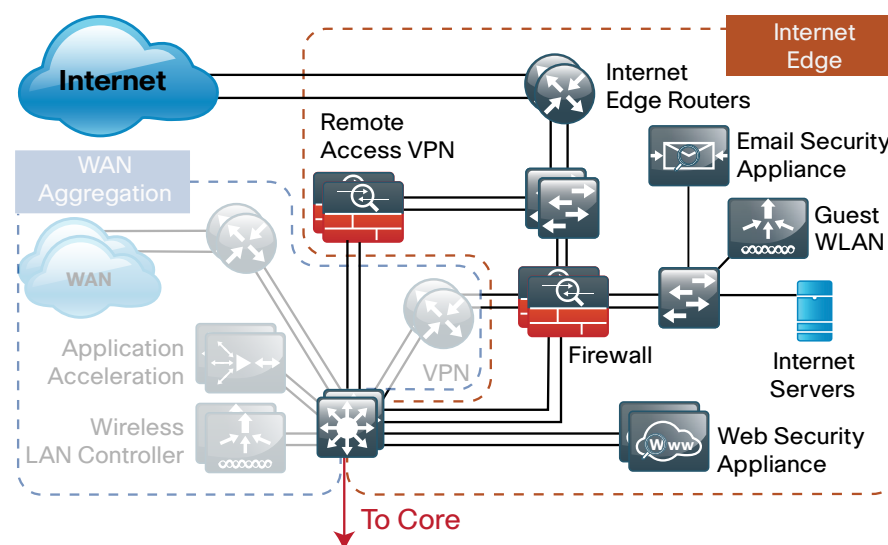
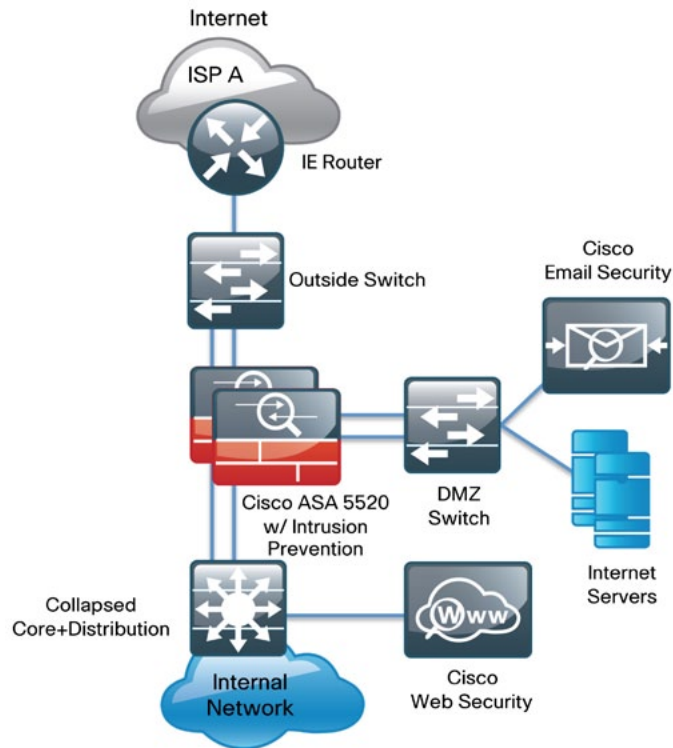
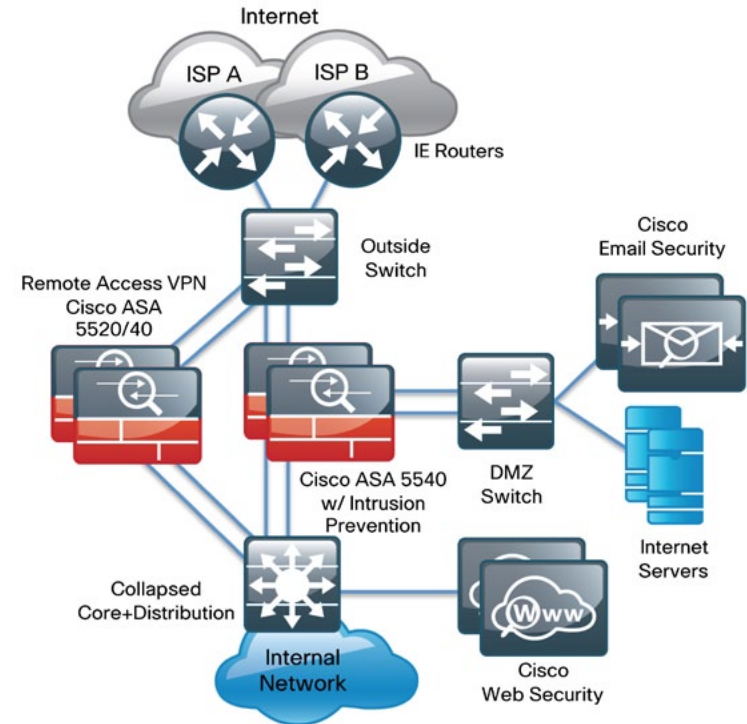


Figure 3. Internet Edge 5K and 10K Designs



The primary difference between the two designs is scale, performance, and resilience. The Internet Edge 5K design is typical for an agency with up to 5000 connected users while the Internet Edge 10K design is for agencies with 5000 to 10,000 connected users. These differences range from the obvious, numbers of users supported by the devices deployed, to how the agency connects to the Internet, with either one or two ISPs. To



accommodate these requirements, each module of the Internet Edge is independent of the others, and an agency can mix and match the different design components to best meet their agency requirements. For example, an agency with fewer than 5000 users might choose to use the Internet Edge 10K design for remote access if they have a highly mobile workforce and their remote access requirements are higher than average.

Internet Edge Connectivity

Agency Overview

Demand for Internet connectivity has increased steadily over the last few decades; for many agencies, access to Internet-based services is a fundamental requirement for conducting day-to-day activity. Email, web access, remote access VPN, and more recently, cloud-based services are critical functions enabling agencies to pursue their missions. An Internet connection that supports these services must be designed to enable the agency to accomplish its Internet-based mission goals.

Three factors define the operational requirements for an agency's Internet connection:

- Value of Internet-based operational activity:
 - revenue realized from Internet operations
 - savings realized by Internet-based services
- Revenue impact of loss of Internet connectivity
- Capital and operational expense of implementing and maintaining various Internet connectivity options

The agency must identify and understand its Internet connection requirements in order to effectively meet the demands of Internet-based operational activity.

Technology Overview

Agencies have come to rely heavily on Internet services such as email, web access, remote access VPN, and B2B service connections. Internet connection speed, availability, and address space requirements are criteria that will shape an Internet connection design. The Internet connection must be able to accommodate an agency's requirements for data volume to the Internet, offer sufficient resiliency to meet service-level agreements, and provide sufficient IP address space to accommodate both Internet-facing and Internet-based services.

An agency's IT staff needs to address three main requirements when designing and implementing an Internet Edge architecture:

- **Connectivity speed:** what is the expected throughput required? Are short bursts of high-volume traffic expected?
- **IP Address space:** A small agency or one that does not rely heavily on web-based services to the Internet will have a different IP space requirement than a large agency that depends heavily on email, remote-access VPN, and content or cloud-based services offered to the Internet.
- **Availability:** Connection speed is only part of the equation; if connectivity must be maintained when the primary Internet connection fails, then the design must offer a resilient Internet connection via a secondary Internet connection.

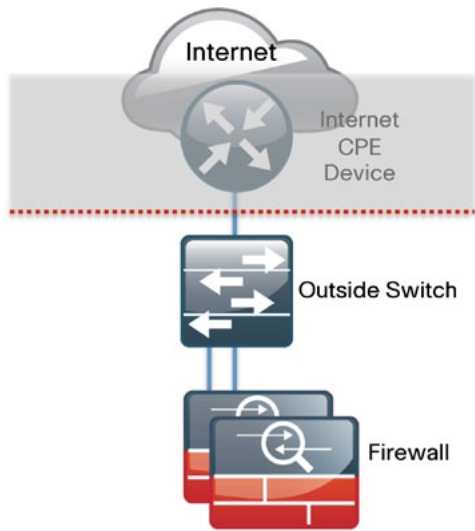
Two design options are described in this guide; the first design, Internet Edge 5K, offers a single connection to one ISP; the second design, Internet Edge 10K, provides a fault tolerant configuration with dual Internet connections. In the Internet Edge 10K design, one connection acts as the primary Internet connection and the second acts as a backup connection in the event that Internet access through the primary connection is lost.

Configuration Overview

Connecting to the Internet

Internet connectivity options vary widely by geographic region and service provider. An agency may be able to choose between cable, DSL, leased line, or Ethernet for the physical connection to the Internet. A common denominator of Internet connectivity is the Ethernet connection to the customer-premises equipment (CPE) device (cable modem, T1 CPE router, etc.), and this is assumed as the demarcation for this design (Figure 4).

Figure 4. Internet Connectivity



Agencies deploying the Internet Edge 5K or 10K designs typically fall into the following Internet connection speed ranges:

Table 1. Internet Connection Speed Requirements

Number of Connected Users	Internet Connection Speed
2000 to 4500	20–50 Mbps
3000 to 7000	35–75 Mbps
6000 to 10,000	70–130 Mbps

If the operational needs include WAN connectivity to connect geographically diverse sites, a cost savings can be realized by combining WAN and Internet connectivity over the same service. A service provider may offer hardware to terminate WAN/Internet connectivity on premise and manage

the Internet/WAN connection device. Provider-supplied hardware and service offerings may reduce operational burden, however, the impact of configuration change lead times and configuration flexibility must be assessed.

The recommendations for Internet access platform selection are:

Table 2. Internet Access Platform Recommendations

Platform	Internet Connection Speed
3925	Up to 100 Mbps
3945	75 to 150 Mbps

Design and configuration discussions for this guide begin at the Ethernet handoff on the outside switch in the Internet edge regardless of how access is delivered.

HA Overview

The decision to use a single or dual Internet connection is based on an agency’s connection availability requirements. If a loss of Internet access will cause an interruption in operations greater than the cost of a backup Internet connection, then the Internet Edge 10K design should be used. A backup Internet connection will assure continued Internet access in the event of a failure to the primary Internet connection, although some services may experience a temporary outage during the switch to the backup link. Most outbound services should be available in a few seconds. The Internet Edge 10K provides:

- Resilient outbound Internet access and inbound email services.
- Additional inbound services can be provisioned to recover in the event of a failure, although some services may experience longer outages.
- Inbound web service does not have seamless failover protection and requires user interaction to point the DNS records at the alternate IP address on the secondary ISP. To achieve higher web-service availability, an agency can host its web service at a colocation facility or use a fully redundant BGP design that advertises the same IP address out to different ISPs. Agencies with services that require a very high level of Internet availability should consider hosting these services at a provider’s Internet colocation facility.

Internet Routing

There are a variety of ways to control routing to and from the Internet. Border Gateway Protocol (BGP) and other dynamic routing options offer various methods to influence Internet routing, but for the majority of agencies with 2000 to 10,000 connected users, a static default route is adequate to establish access to the Internet and has the least operational complexity. If an agency's routing requirements exceed what can be addressed by static routing, the Cisco Enterprise Internet Edge Design Guide (http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/IE_DG.html) covers more complex Internet connectivity deployments.

Active/Standby vs. Active/Active Internet Connectivity

The Internet Edge 10K is a resilient design with primary and backup Internet connections. If Internet access via the primary link is lost, the design will automatically fail over to the secondary link. This configuration is sufficient for agencies of 2000 to 10,000 connected users who are not hosting critical content or eCommerce in their DMZ. This design uses ICMP probes to an Internet IP address from the Cisco Adaptive Security Appliances (ASAs) firewalls. When the ASA firewall stops getting responses to the probes, it will fail over to the secondary link. This resilient design offers a simple but effective solution to maintain Internet access for users, and Internet mail (with an appropriately configured DNS). Further detail on configuration of this capability will be addressed in the 'Firewall' and 'Remote Access VPN' sections of this document.

The design does not address multi-homed routing options, e.g., using BGP with multiple Internet connections to multiple ISPs. Refer to the Cisco Enterprise Internet Edge Design Guide (http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/IE_DG.html) for more information on multi-homed Internet connectivity designs.

Notes

Firewall

Agency Overview

The Internet edge is the point where the agency's network connects to the Internet. This is the perimeter of the network, where a line is drawn between the public Internet and the private resources contained within an agency's network. Worm, virus, and botnet infiltration pose substantial threat to network performance, availability, and data security. To add to these problems, an agency's Internet connection can contribute to employee productivity loss and leakage of confidential data.

Network security, as applied at the firewall, must assure that the agency's data resources are protected from snooping and tampering, and prevent compromise of hosts by resource-consuming worms, viruses, and botnets. Additionally, the firewall policy must establish the appropriate balance to provide security without interfering with access to Internet-based applications, or hindering connectivity to agency partners' data via extranet VPN connections.

Technology Overview

Internet-based attackers are a threat to an agency's network infrastructures and data resources. Most networks connected to the Internet are subject to a constant barrage of worms, viruses, and targeted attacks. Agencies must be vigilant in protecting their network, user data, and customer information. Additionally, most network addresses must be translated to an Internet-routable address and the firewall is the logical place for this function.

Firewall security is an integral part of every Internet Edge deployment today—to protect information while meeting the need for secure reliable networks, and to enforce policy to maintain employee productivity. Where industry regulations apply, firewalls play a crucial role in an agency's ability to address regulatory compliance requirements. Regulatory requirements vary by country and industry; this document will cover specific regulatory compliance requirements.

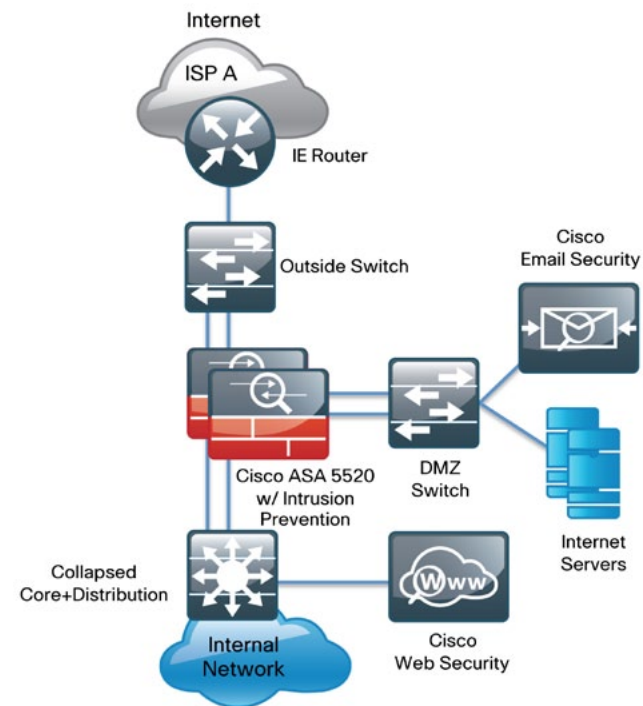
The Cisco Adaptive Security Appliance (ASA) firewall family sits between the agency's internal network and the Internet and is a fundamental infrastructural component that minimizes the impact of network intrusions while maintaining worker productivity and data security.

This design uses Cisco ASA 5500s for Internet Edge firewall security. They are configured in an active/standby pair for high availability to ensure that Internet access is minimally impacted by firewall software maintenance or hardware failure. The Cisco ASAs are configured in routing mode. They apply NAT and firewall policy, and host IPS-SSMs to detect and mitigate malicious or harmful traffic.

Two deployment options are discussed to address Internet access requirements for high availability and to meet operational requirements for device-level separation between Remote Access VPN and Firewall:

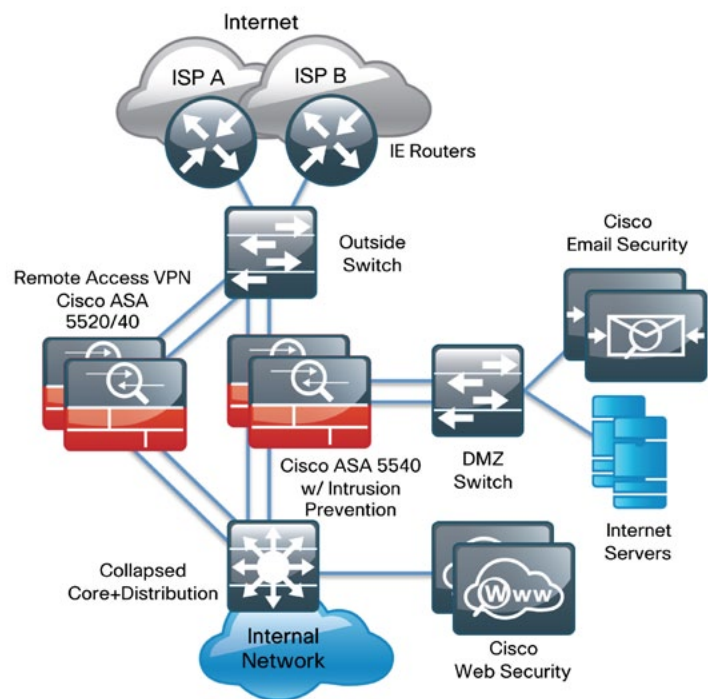
- The Internet Edge 5K firewall design uses a single Internet connection, and integrates the Remote Access VPN function in the same ASA pair that provides firewall (Figure 5):

Figure 5. Internet Edge 5K Topology



- The Internet Edge10K firewall design uses dual Internet connections for resilient access to the Internet. Remote Access VPN is provided by a separate pair of ASAs, to provide additional scalability and operational flexibility (Figure 6):

Figure 6. Internet Edge 10K Topology



A good portion of the configuration described in this section is common to both the Internet Edge 5K and Internet Edge 10K designs. If a section describes configuration that is specific to the Internet Edge 5K or Internet Edge 10K design, this will be specifically mentioned in that section. The configurations would be valid for any of the one-rack-unit ASA security appliances, although the interface names described in the configuration examples need to be modified slightly to address the Fast Ethernet interfaces available on the ASA 5510.

Hardware applied in this design is selected based on the following performance values:

Table 3. Cisco ASA Family Device Performance

Cisco ASA Family Product	Throughput
Cisco ASA 5510	300 Mbps
Cisco ASA 5520	450 Mbps
Cisco ASA 5540	650 Mbps

The firewall configuration process consists of the following procedures:

Process

1. Basic Connectivity Configuration
2. Inside Routing Configuration
3. Firewall Logging and Monitoring Configuration
4. Firewall Remote Management Configuration
5. Firewall Internet Connectivity Configuration
6. Firewall De-Militarized Zone Configuration
7. Firewall Address Translation (NAT/PAT) Configuration
8. Blacklist Policy Configuration for inside hosts' access to the Internet
9. Whitelist Policy Configuration for Internet access to Web and Email DMZ hosts
10. High Availability Configuration

Firewall Configuration Details

The Cisco ASA can be configured from the command line or from the graphical user interface, Cisco Adaptive Security Device Manager (ASDM). If ASDM is the preferred method for device configuration, the appliance's default configuration offers a DHCP scope and management interfaces on the 'management' interface:

```
interface management 0/0
ip address 192.168.1.1 255.255.255.0
nameif management
security-level 100
no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

Connect the Cisco ASA's management port directly to a PC or to an Ethernet switch, and connect a host with a Java-enabled web browser to the same VLAN on the switch.



Tech Tip

If connecting to an Ethernet switch, make sure that the switch is not connected to the production network or on a VLAN with an existing DHCP server as the ASA will serve DHCP.

Access the device's management URL, <https://192.168.1.1/>, and browse the configuration. If command-line interface is preferable, the Cisco ASA CLI is available via telnet or SSH, or may be accessed via serial connection to the console port.

Only one of the two ASAs in the HA pair needs to be configured as the secondary Cisco ASA will replicate the primary Cisco ASA's configuration when the two devices synchronize their configuration. The last step of the configuration will set up high availability and synchronize the configurations and session activity.

Procedure 1 Basic Connectivity Configuration

To get the Firewall up and running, a few basic parameters must be configured: the inside interface's address must be defined, and basic routing must be set up.

Procedure steps:

1. Configure device identity values (hostname and domain name)
2. Define connectivity to inside network
3. Connect inside interface to the adjacent distribution switch



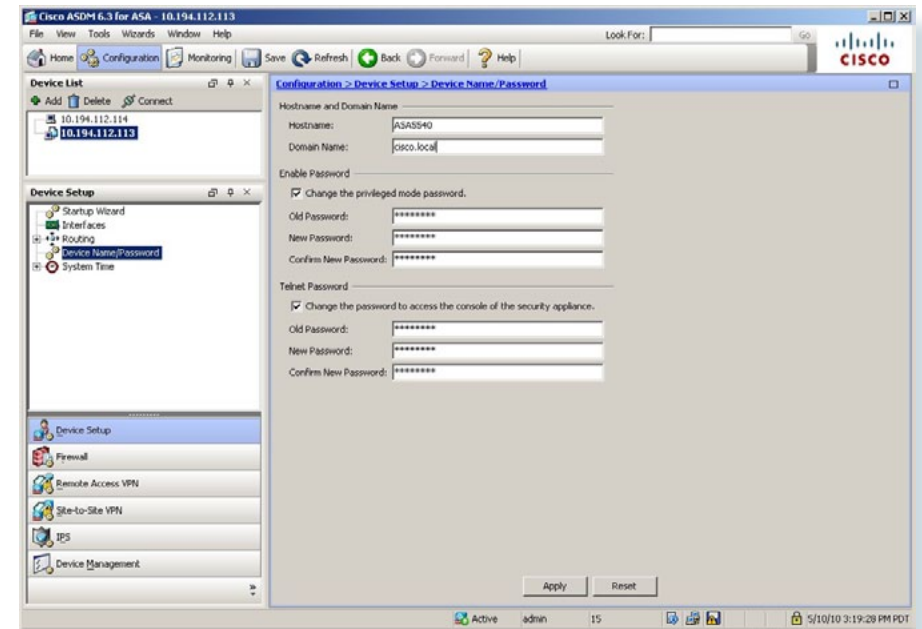
Tech Tip

IP addresses and interface names in this example are specific to the Cisco lab testing environment, values in an actual deployment will likely be different.

Step 1: Browse to **Device Setup > Device Name/Password**. Configure the Cisco ASA's host and domain name and set the enable password (Figure 7).

To simplify troubleshooting, the host and domain name will match the outside DNS name and IP address of the firewall, particularly if the firewall's outside interface will accept remote-access VPN connections.

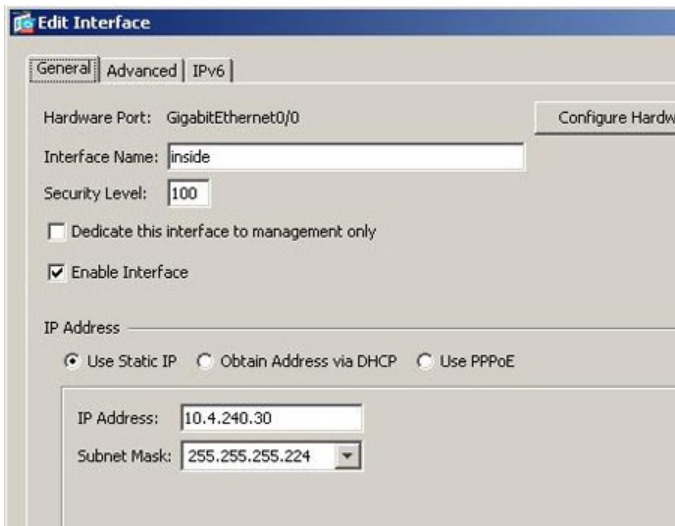
Figure 7. Configure Hostname and Passwords



Step 2: Define the firewall's IP connectivity to the 'inside' network on the GigabitEthernet0/0 interface by browsing to **Device Setup > Interfaces** (Figure 8).

All interfaces on the ASA must have a security-level setting. The security level denotes an interface's security relative to other interfaces; clients on a higher security interface can connect to hosts on a lower security interface by default. Inside interfaces are assigned security level 100, the highest value, while outside interfaces are assigned security level 0, the lowest value. The ASA recognizes the interface names "outside" and "inside", and applies the default security-level configurations. Interfaces may be configured for any security level; this configuration will be discussed in the 'De-Militarized Zone' section.

Figure 8. Interface Configuration Detail



Step 3: Connect the Cisco ASA's 'inside' interface to the appropriate distribution switch port.

The 'inside' GigabitEthernet port on the ASA connects to a VLAN access port on the Internet Edge/WAN distribution switch or collapsed core/distribution switch. Define the appropriate access VLAN configuration on the adjacent inside switch(es) that the ASAs connect to:

```
interface GigabitEthernet3/0/10
description ASA5540
switchport access vlan 300
spanning-tree link-type point-to-point
```

Executing the preceding steps in ASDM will apply the following CLI configuration:

```
hostname [ASA5540]
domain-name [cisco.local]
enable password [password]
passwd [password]
interface GigabitEthernet0/0
nameif inside
security-level 100
ip address 10.4.240.30 255.255.255.224 standby 10.4.240.29
no shutdown
```

Procedure 2 Inside Routing Configuration

The ASA exchanges routing information via EIGRP dynamically on the 'inside' network to simplify the routing configuration. Changes to the campus and WAN networks' addressing or topology should not require routing configuration changes on the ASA.

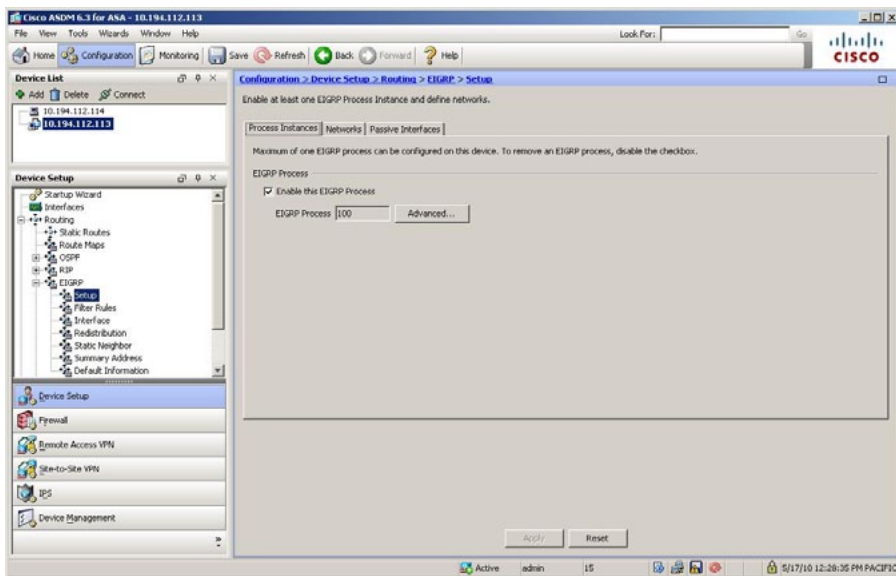
Procedure steps:

1. Define EIGRP process number
2. Define networks to be included in EIGRP updates
3. Restrict EIGRP activity to specific interfaces
4. Define static route redistribution

Step 1: Define the ASA's EIGRP process number in the **Device Setup > Routing > EIGRP > Setup** panel (Figure 9).

The ASA must be configured in the same EIGRP process as the other devices it is expected to exchange routing information with.

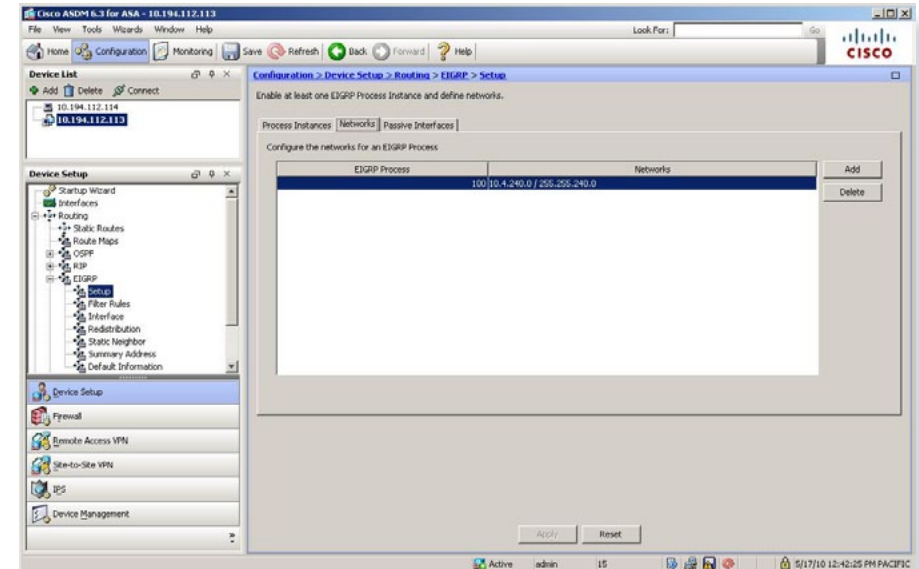
Figure 9. Define EIGRP Process



Step 2: Configure the network subnets where the ASA will exchange routes. This configuration is found on the 'Networks' tab in the **Device Setup > Routing > EIGRP > Setup** panel.

The 'Networks' configuration should not include the outside subnets. Apply a subnet number that encompasses all of the inside and DMZ subnets to reduce the amount of configuration needed to apply to establish dynamic route configuration (Figure 10). If the networks cannot be easily summarized, all interfaces except for the outside interface can be entered separately.

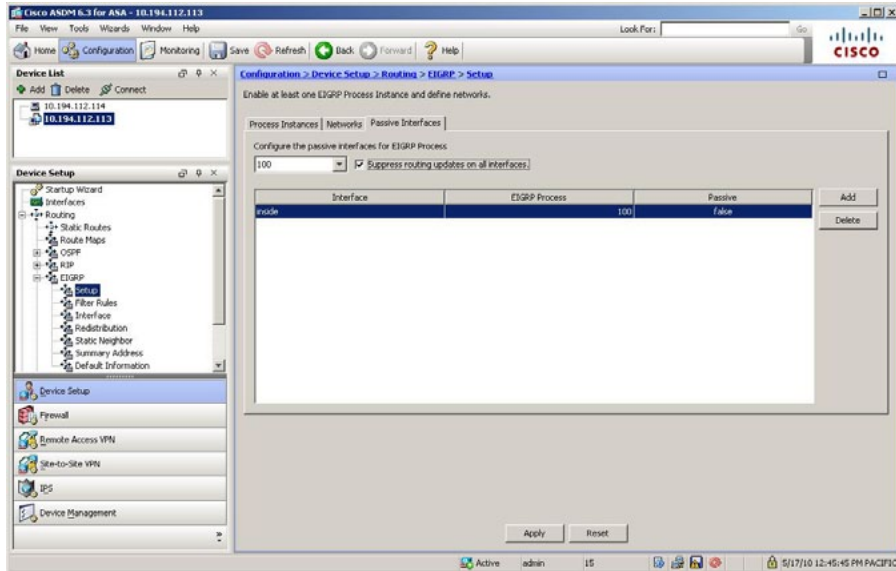
Figure 10. Configure EIGRP Networks



Step 3: Configure EIGRP passive-default and enable route advertisements only on the inside interface. This configuration is found on the 'Passive Interfaces' tab in the **Device Setup > Routing > EIGRP > Setup** panel (Figure 11).

All the interfaces except the inside interface are set to "passive"; this is so they will not exchange routes on public interfaces. There are no other routers the ASA needs to exchange routing information with and advertising internal routing information to less secure networks is not recommended.

Figure 11. Define Passive-Default



Step 4: Configure EIGRP to redistribute static routes. This configuration is found on the **Device Setup > Routing > EIGRP > Redistribution** panel (Figure 12).

The ASA redistributes static routes, which allows the ASA to advertise a default route to the rest of the network. If a specific network (that is not encompassed by summary routes from the core) cannot be accessed, the traffic will follow the default route to the ASA and it will send the traffic out to the Internet.

Figure 12. Define Static Route Redistribution



Executing the preceding steps in ASDM will apply the following CLI configuration:

```
router eigrp 100
  no auto-summary
  network 10.4.240.0 255.255.255.240
  passive-interface default
  no passive-interface inside
  redistribute static
```

Procedure 3 Logging and Monitoring Configuration

Logging and monitoring are critical aspects of network security devices to support troubleshooting and policy compliance auditing.

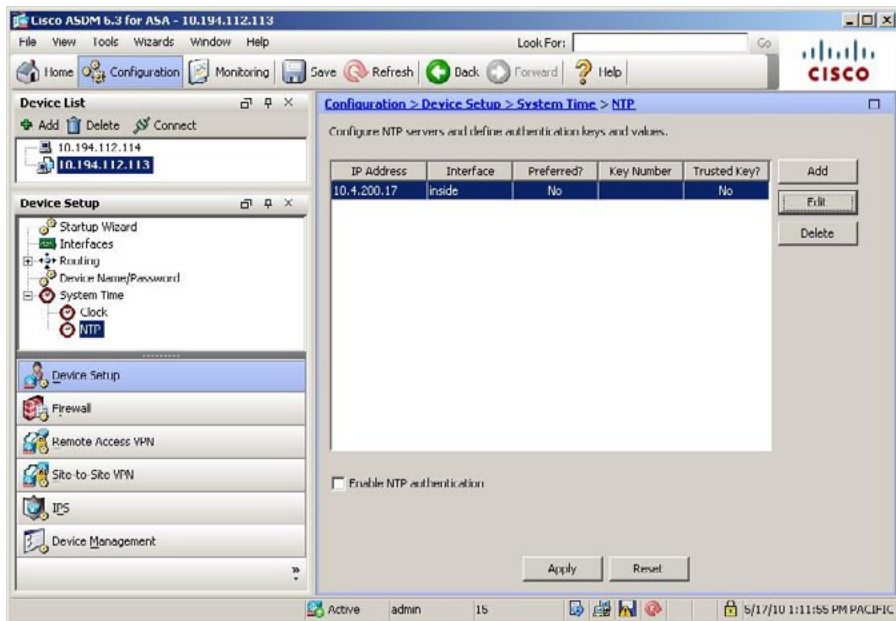
Procedure steps:

1. Configure network time synchronization
2. Enable logging
3. Define logging parameters and behavior
4. Configure log server addresses
5. Enable SNMP management

Step 1: Configure network time synchronization in the **Device Setup > System Time > NTP** panel (Figure 13).

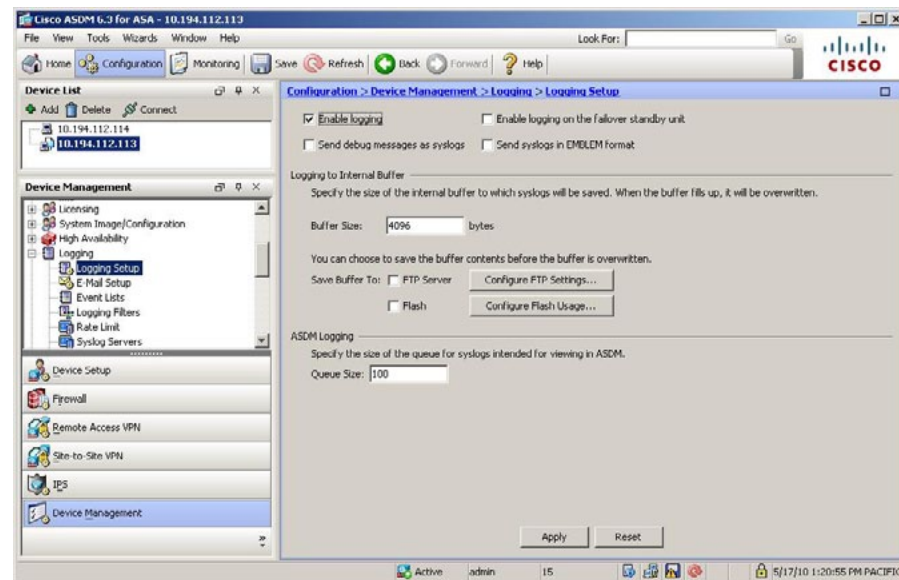
Firewalls need accurate time for network-activity logging. By synchronizing the firewall to a network time source, the firewall will be synchronized to the same time as other network devices and NTP time servers.

Figure 13. NTP Configuration



Step 2: Check the 'Enable logging' checkbox in **Device Management > Logging > Logging Setup** (Figure 14).

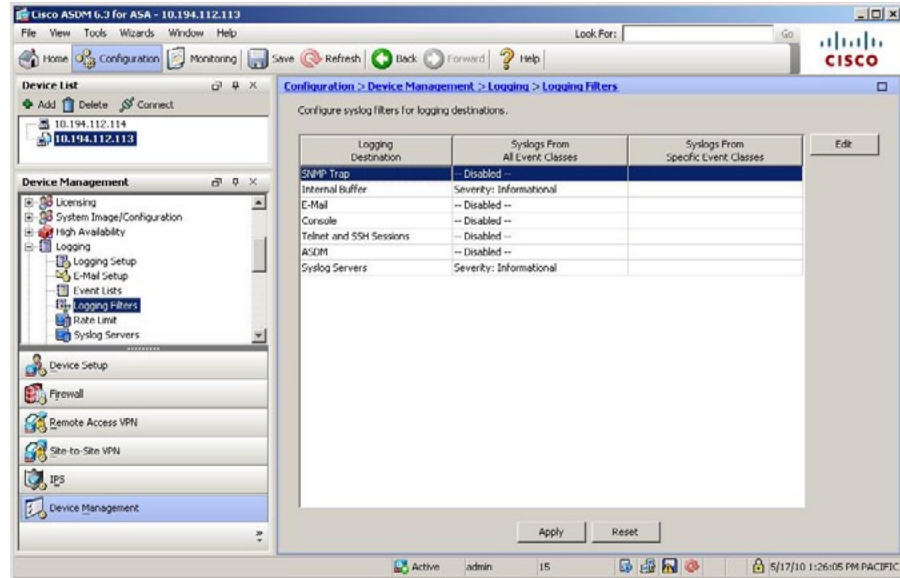
Figure 14. Enable Logging



Step 3: Configure the 'Internal Buffer' and 'Syslog Server' log filters to 'Severity: Informational' in the **Device Management > Logging > Logging Filters** panel (Figure 15).

Informational-level logging provides the ideal balance between detail and log-message volume. Lower log levels produce less messages, but not enough detail to effectively audit network activity. Higher log levels produce a larger volume of messages, but do not add sufficient value to justify the number of messages logged.

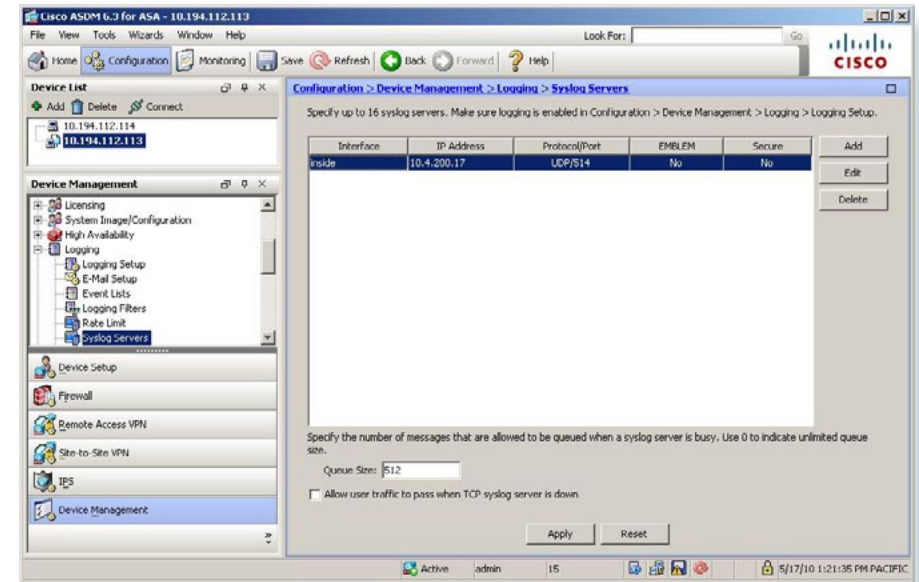
Figure 15. Define Logging Filters



Step 4: Configure syslog server addresses in **Device Management > Logging > Syslog Servers** (Figure 16).

Syslog transmits status updates and firewall policy activity to a log server. This is useful for network diagnostics and policy compliance review.

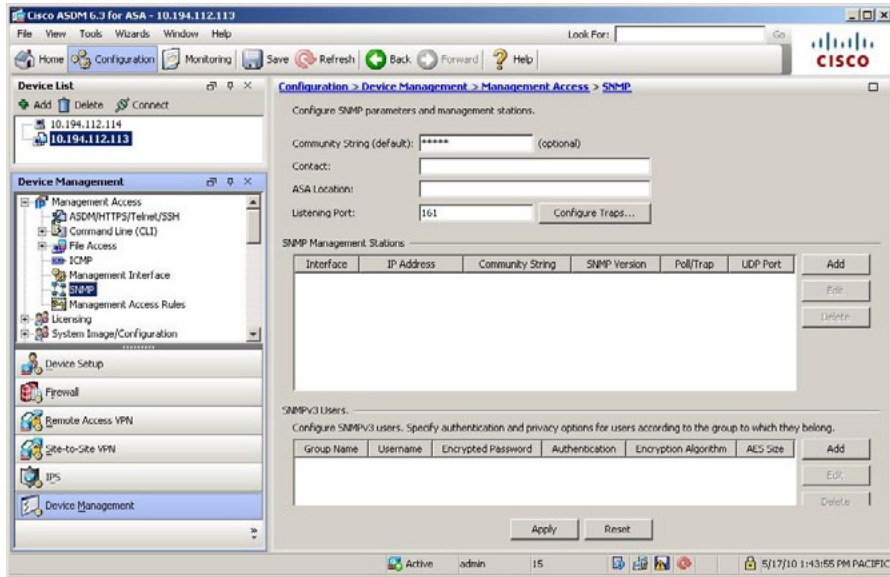
Figure 16. Configure Logging Servers



Step 5: Configure the SNMP community string and additional configuration in **Device Management > Management Access > SNMP** (Figure 17).

Specify the IP address of the SNMP manager and whether it will poll the ASA for values, or if it will receive traps. This configuration provides the capability for SNMP management tools to access statistics on the device.

Figure 17. Configure SNMP Values



Executing the preceding steps in ASDM will apply the following CLI configuration:

```
ntp server [10.4.200.17]
logging enable
logging trap informational
logging buffered informational
logging host inside [10.4.200.17]
snmp-server community Cisco
snmp-server host inside [finish configuration][poll | trap]
[version]
snmp-server enable
```

Procedure 4 Remote Management Configuration

After the initial setup of the ASA, remote management access is available for convenient configuration, management, and troubleshooting. The following configuration allows for remote connectivity from any internal network via HTTPS or SSH.

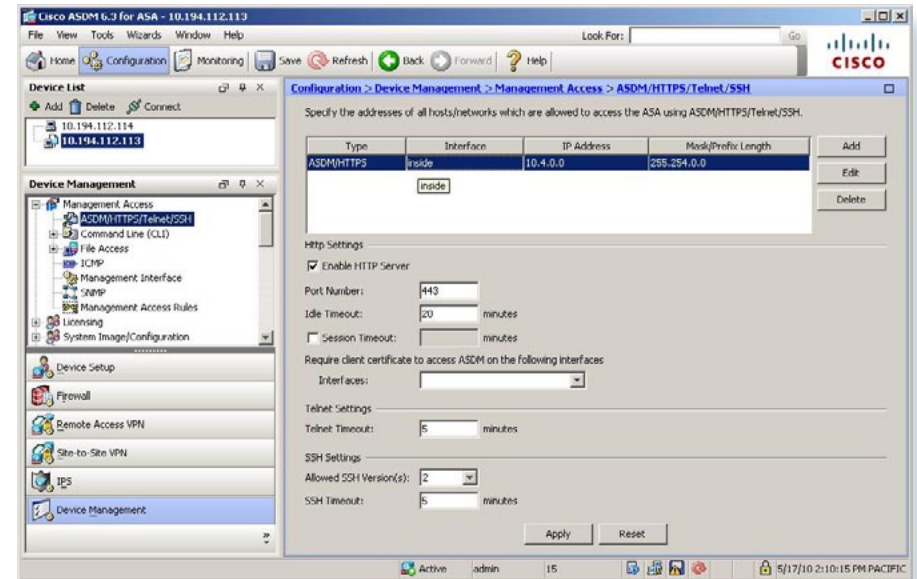
Procedure steps:

1. Enable HTTP server
2. Define SSH access
3. Configure local username and password for administrative access
4. Add AAA-based administrative access

Step 1: Enable the HTTP server for the inside networks in the **Device Management > Management Access > ASDM/HTTPS/Telnet/SSH** panel (Figure 18).

ASDM requires that the ASA's HTTP server be available. Be sure that the configuration includes networks where administrative staff will access the device through ASDM; the ASA can offer controlled ASDM access for a single address or management subnet by changing the network statements below.

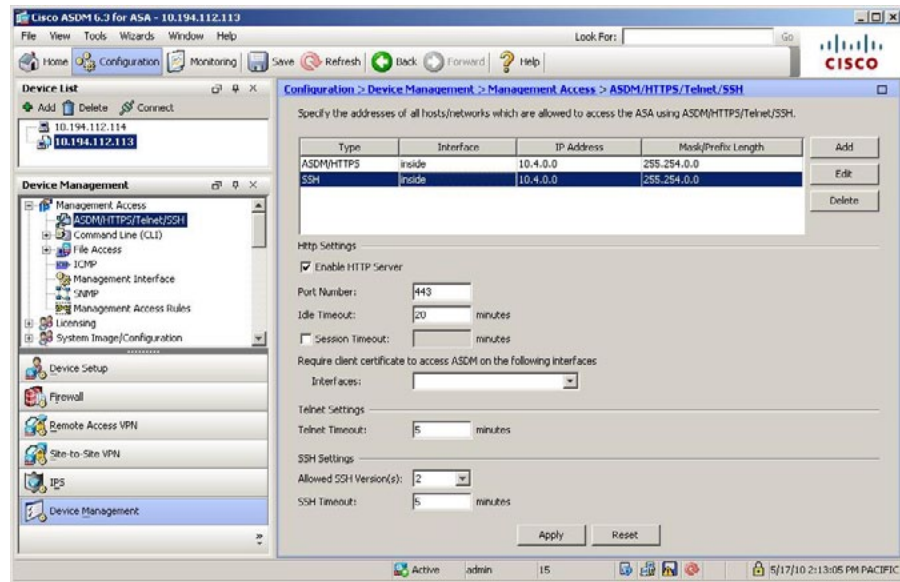
Figure 18. Enable ASDM Access



Step 2: Enable the SSH server for the inside networks in the **Device Management > Management Access > ASDM/HTTPS/Telnet/SSH** panel (Figure 19).

Telnet is not recommended for management because traffic is sent over the network without encryption.

Figure 19. Add SSH Access



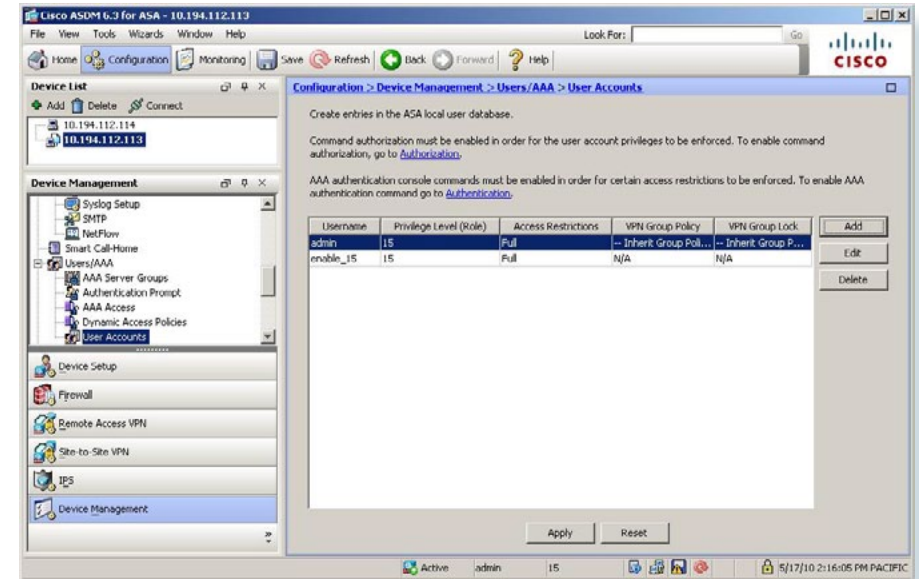
If the CLI is used to configure the Cisco ASA, RSA keys must be generated manually to enable SSH functionality:

```
crypto key generate rsa
```

Step 3: Configure a local username and password in **Device Management > Users/AAA > User Accounts** panel (Figure 20).

A local username for device access is valuable in the event the authentication resources (AAA, AD, etc.) are unavailable.

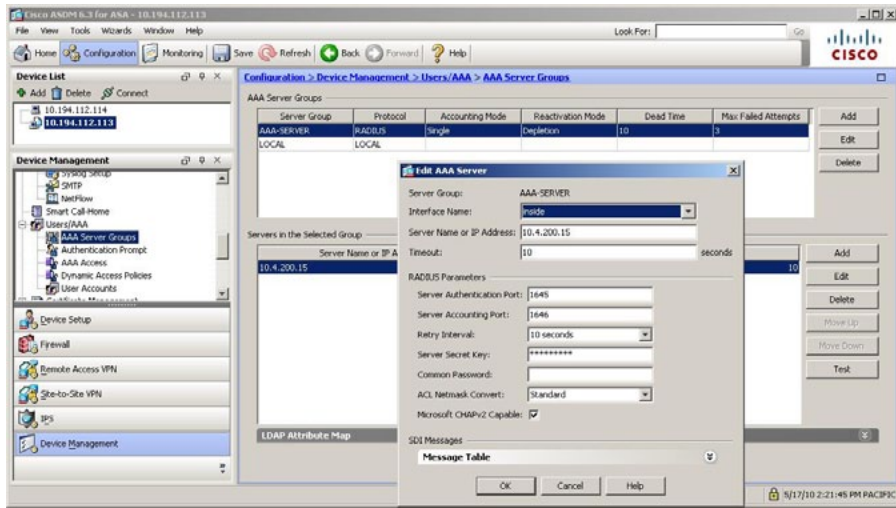
Figure 20. Configure Local Usernames



Step 4: Configure the ASA to authenticate management access with a AAA server in the **Device Management > Users/AAA > AAA Server Groups** panel (Figure 21).

Administrative access is authenticated with a RADIUS server. In the Remote Access VPN section, a separate server group will be configured that uses LDAP (Microsoft Active Directory) for the authentication/authorization backend, in order to leverage an agency's existing user directory.

Figure 21. Configure AAA Servers



Executing the preceding steps in ASDM will apply the following CLI configuration:

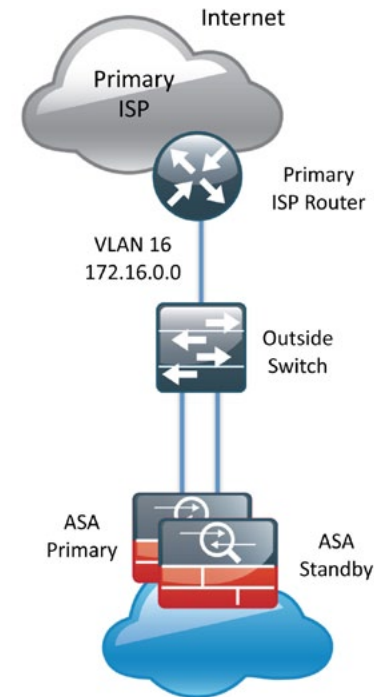
```
http server enable
http 10.4.0.0 255.254.0.0 inside
ssh 10.4.0.0 255.254.0.0 inside
ssh version 2
username admin password [password] privilege 15 aaa-server
AAA-SERVER protocol radius
aaa-server AAA-SERVER (inside) host 10.4.200.15
key [SecretKey]
aaa authentication enable console AAA-SERVER LOCAL
```

Procedure 5 Firewall Internet Edge Configuration

Internet connectivity varies based on the agency's availability requirement for Internet access. Two options are available:

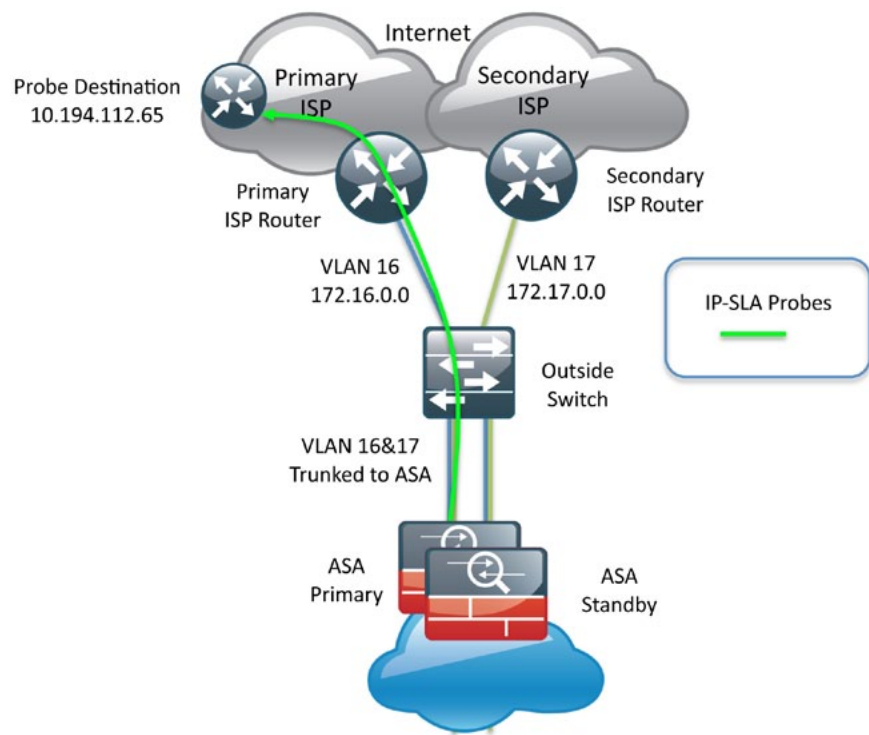
- Internet Edge 5K uses a single Internet connection via one router that carries the Internet traffic (Figure 22)

Figure 22. Internet Edge 5K ISP Connectivity



- Internet Edge10K uses dual Internet connections via two routers that carry the Internet traffic (Primary Internet Customer Premise Equipment ['Internet CPE-1'] and Secondary Internet Customer Premise Equipment ['Internet CPE-2']) (Figure 23).

Figure 23. Internet Edge 10K ISP Connectivity



NOTE: IP addresses and interface names in this example are specific to the Cisco lab testing environment, values in an actual deployment will likely be different.

Internet Edge 5K Outside Routing Configuration

If high availability for Internet access is not required (Internet Edge 5K design), the ASAs' GigabitEthernet 0/3 is the outside interface and is connected through a switch to the Internet CPE.

Procedure steps:

1. Connect the outside interface to a switch via the appropriate VLAN.
2. Configure outside IP address.
3. Define outside default route.

Step 1: Connect the Cisco ASA's GigabitEthernet 0/3 to the adjacent switch, which is also connected to the ISP router. If more than one VLAN is used on the 'outside' switch, be sure that the ASA's switch port is configured in the same VLAN as the Internet CPE.

Step 2: Configure the GigabitEthernet 0/3 interface that will be used for the outside connection. When 'nameif outside' is configured, the interface's security level will be automatically set to 0.

Step 3: Assign the default route to the Internet CPE's address.

Executing the preceding steps in ASDM will apply the following CLI configuration:

```
interface GigabitEthernet0/3
nameif outside
security-level 0
ip address 172.16.130.125 255.255.255.128 standby
172.16.130.124
route outside 0.0.0.0 0.0.0.0 172.16.130.126 1
```

Internet-10K Outside Routing Configuration

If resilient Internet access is required, the Internet 10K design, the ASAs' GigabitEthernet 0/3 is configured as a VLAN trunk to the outside switch, which separates the VLANs to the appropriate routers, Internet CPE-1 and Internet CPE-2.

Procedure steps:

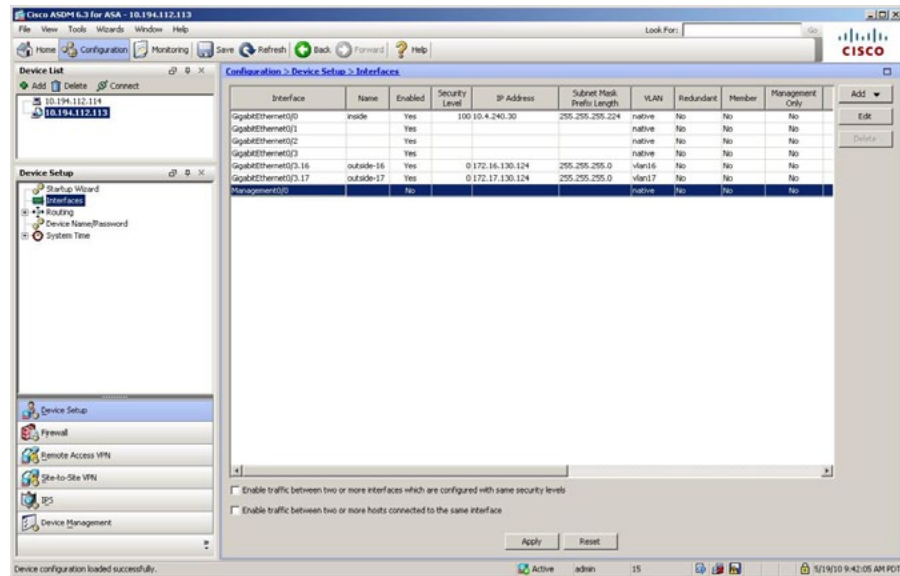
1. Connect the outside interface to a switch via the appropriate VLAN.
2. Configure outside IP address.
3. Define primary outside default route with object-tracking.
4. Define secondary outside default route
5. Define a static host route for the tracked object.
6. Verify that the tracked object is working

Step 1: Connect the Cisco ASA's GigabitEthernet 0/3 to the adjacent switch, which is also connected to the ISP router. If more than one VLAN is used on the 'outside' switch, be sure that the ASA's switch port is configured in the same VLAN as the Internet CPE.

Step 2: Configure the GigabitEthernet 0/3 interface that will be used for the outside connection (Figure 24).

A VLAN trunk connects the ASA to the outside switch. Two subinterfaces are configured for two VLANs, one for each connection to the upstream Internet routers, Internet CPE-1 and Internet CPE-2.

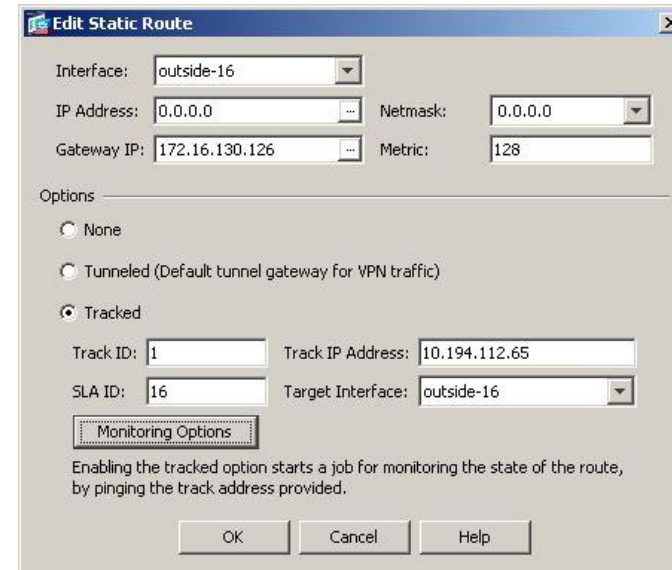
Figure 24. Internet Edge-10K Outside Interface Configuration



Step 3: Define the primary route to the two Internet CPE addresses and configure object-tracking on the route by clicking 'Add' in the **Device Setup > Routing > Static Routes** panel (Figure 25).

The primary route will carry a metric of 1, making the route preferred; the primary route's availability is determined by the state of the 'track 1' object that is appended to the primary route. The route-tracking configuration defines a target in ISP-1's network that the ASA will send ICMP probes (pings) to determine if the network connection is active or not. The target is an object on the primary service provider's network, such as an intermediate router that can be discovered with traceroute.

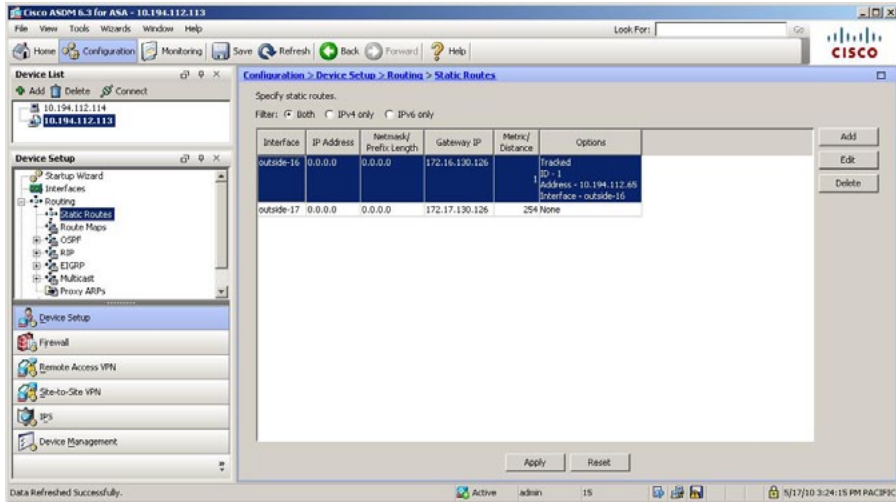
Figure 25. Tracked Route Configuration



Step 4: Configure the secondary route, also in the **Device Setup > Routing > Static Routes** panel (Figure 26).

The secondary route carries a metric of '254' so that the ASA will only use the route when the primary route is unavailable.

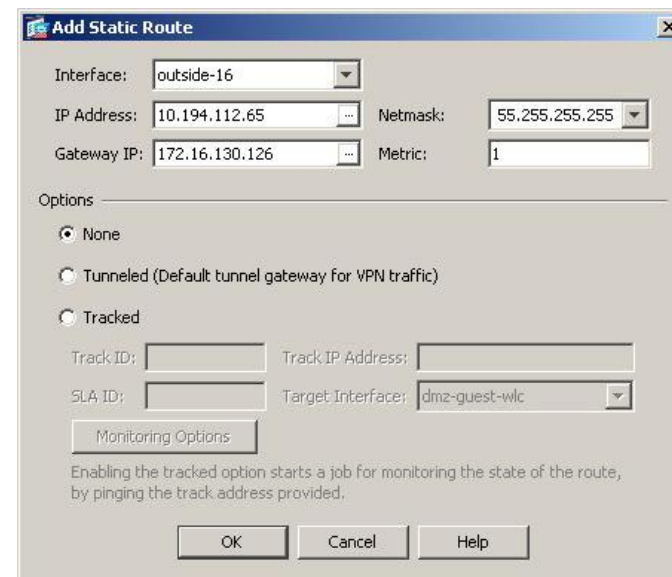
Figure 26. Add Route for Secondary ISP Connection



Step 5: Still in the **Device Setup > Routing > Static Routes** panel, add a host route for the tracked object via the Internet-CPE-1 address. This will assure that probes to the tracked object will always use the ISP-1 connection (Figure 27).

The tracked object should be in the primary Internet Service Provider's network. The point of tracking an object in the primary ISP's network is because if reachability to this object is available, then all connectivity to that point is working: the ASA's connection to the customer premise router, the WAN connection, and most routing inside the ISP's network. If the tracked object is unavailable, it is likely that the path to the primary ISP is down and the ASA should prefer the secondary ISP's route.

Figure 27. Add Host Route for Tracked Object



Step 6: Verify that the tracked object is reachable with the 'show track' command on the ASA CLI:

```
ASA5540# show track
Track 1
  Response Time Reporter 16 reachability
  Reachability is Up
  14 changes, last change 2d02h
  Latest operation return code: OK
  Latest RTT (milliseconds) 1
  Tracked by:
    STATIC-IP-ROUTING 0
```

Executing the preceding steps in ASDM will apply following CLI configuration:

```
interface GigabitEthernet0/3
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/3.16
vlan 16
nameif outside-16
security-level 0
ip address 172.16.130.124 255.255.255.128 standby
172.16.130.123
!
interface GigabitEthernet0/3.17
vlan 17
nameif outside-17
security-level 0
ip address 172.17.130.124 255.255.255.128 standby
172.17.130.123
!
route outside-16 0.0.0.0 0.0.0.0 172.16.130.126 1 track 1
sla monitor 16
  type echo protocol ipIcmpEcho 10.194.112.65 interface
  outside-16
  num-packets 3
  frequency 10
sla monitor schedule 16 life forever start-time now
!
track 1 rtr 16 reachability
route outside-17 0.0.0.0 0.0.0.0 172.17.130.126 254
route outside-16 10.194.112.65 255.255.255.255 172.16.130.126
```

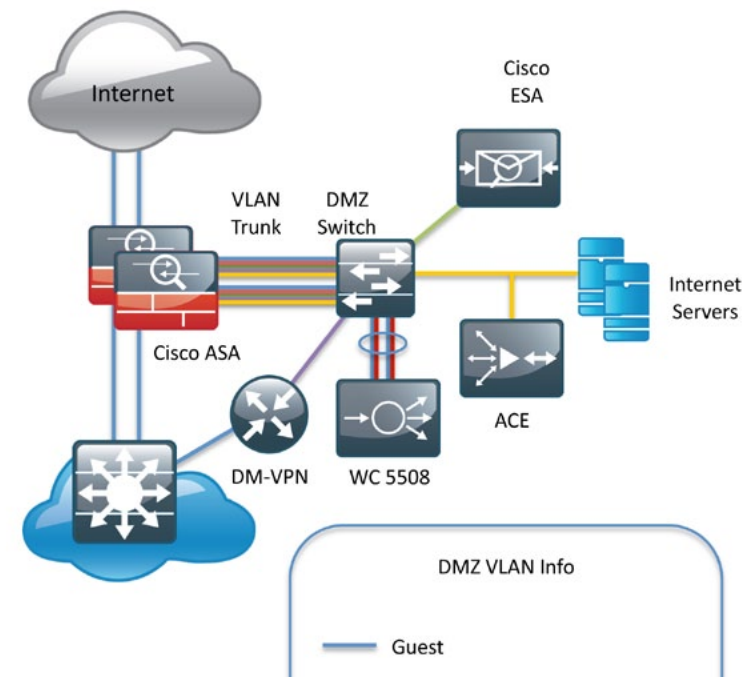
Procedure 6 Firewall De-Militarized Zone Configuration

The Firewall's De-Militarized Zone (DMZ) is a portion of the network where, typically, traffic to and from other parts of the network is tightly restricted. Agencies place network services in a DMZ for exposure to the Internet. These servers are typically not allowed to initiate connections to the 'inside' network, except for specific circumstances.

A DMZ for web and file-transfer servers is configured for Internet-accessible servers to be hosted on site.

The DMZ network is connected to the ASAs on the ASAs' GigabitEthernet interface via a VLAN trunk to allow the greatest flexibility if new VLANs must be added to connect additional DMZs. The trunk connects the ASAs to a 3750G access-switch stack to provide resiliency. The DMZ VLAN interfaces on the Cisco ASA are each assigned an IP address, which will be the default gateway for each of the VLAN subnets. The DMZ switch only offers Layer 2 switching capability; the DMZ switch's VLAN interfaces do not have an IP address assigned, save for one VLAN interface with an IP address for management of the switch (Figure 28).

Figure 28. DMZ VLAN Topology and Services



The number of secure VLANs is arbitrary. This design illustrates an example of one secured network. If multiple types of hosts are to be connected in an Internet-facing DMZ, segmenting the DMZ along functional boundaries may be necessary, particularly since hosts that are exposed to the Internet are vulnerable to compromise, and must not offer a springboard to other hosts. However, traffic between DMZ VLANs should be kept to a minimum. Placing servers that must share data on a single VLAN will improve performance and reduce load on network devices.

Procedure steps:

1. Configure DMZ VLAN Trunk
2. Configure basic DMZ VLAN
3. Configure DMZ trunk switch port
4. Configure DMZ access switch ports



Tech Tip

Setting the DMZ connectivity as a VLAN trunk offers the greatest flexibility.

Step 1: Configure GigabitEthernet 0/1 as the interface that carries the VLAN trunk for the various DMZs (Figure 29).

Values are not assigned for the interface name, security level, or IP address on trunk interfaces.

Figure 29. Define DMZ Trunk Interface

The screenshot shows the 'Edit Interface' window for GigabitEthernet0/1. The 'General' tab is selected. The 'Hardware Port' is set to 'GigabitEthernet0/1'. The 'Interface Name' field is empty. The 'Security Level' field is empty. There is a checkbox for 'Dedicate this interface to management only' which is unchecked, and a checkbox for 'Enable Interface' which is checked. The 'IP Address' section has three radio buttons: 'Use Static IP' (selected), 'Obtain Address via DHCP', and 'Use PPPoE'. Below these, the 'IP Address' field is empty and the 'Subnet Mask' is set to '255.0.0.0'. At the bottom, the 'Description' field contains the text 'dmz trunk to dmz-3750 stack port x/0/1'.

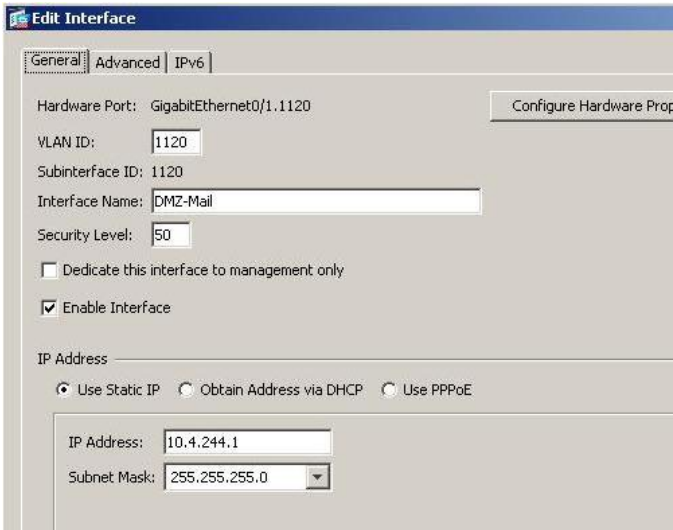
Step 2: Configure the DMZ VLAN connectivity on GigabitEthernet 0/1 subinterfaces (Figure 30).

Each of the various DMZ VLAN interfaces must be configured with appropriate IP addresses for the attached subnet, as well as an intuitive interface name to be used for NAT and security policy configuration. Table 4 illustrates the configuration for one VLAN interface. This design applies several DMZ VLAN interfaces:

Table 4. DMZ Configuration Information

Interface Label	IP Address & Netmask	VLAN	Security Level	Name
GigabitEthernet 0/1.1121	10.4.245.1/24	1120	50	dmz-web

Figure 30. DMZ Sub-Interface Configuration



Step 3: Define the DMZ switch ports that connect to the ASAs as trunk ports and add the appropriate VLANs:

```
interface GigabitEthernet1/0/1
description ASA5540-1 DMZ uplink
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,1121
switchport mode trunk
spanning-tree link-type point-to-point
```

Step 4: Configure DMZ switch ports that connect to DMZ hosts as access ports and assign the appropriate VLANs:

```
interface GigabitEthernet1/0/11
description vpn-7206-1 gig0/3
switchport access vlan 1128
```

Executing the preceding steps in ASDM will apply the following CLI configuration:

```
interface GigabitEthernet0/1
description dmz trunk to dmz-3750 stack port x/0/1
no nameif
no security-level
no ip address
interface GigabitEthernet0/1.1120
vlan 1120
nameif dmz-web
security-level 50
ip address 10.4.245.1 255.255.255.0 standby 10.4.245.2
```

Procedure 7 Address Translation Configuration

Prior to this step, no access from the inside network to the Internet, or from the Internet to the DMZs was possible. This step is required to permit Internet traffic for the inside network and the DMZs; the inside and DMZ networks are numbered using private (RFC 1918) addressing that is not Internet routable, so the ASAs must translate the private addresses to outside Internet routable addresses. For this configuration, all inside addresses are translated to the public address on the outside interface.

NOTE: As the address translation configuration described in this portion of the document is applied, the ASA will apply its default access rule set that permits traffic from higher-security interfaces to lower-security interfaces. Review the expected traffic carefully; if some or all traffic that is allowed by the default rules should not be permitted, shut down the interfaces until the firewall rule set is completely configured.

NAT configuration varies depending on the Internet Edge 5K or Internet Edge 10K design. Most of the configuration is common to either design, although some steps must be duplicated to configure both outside interfaces in the Internet Edge 10K design.

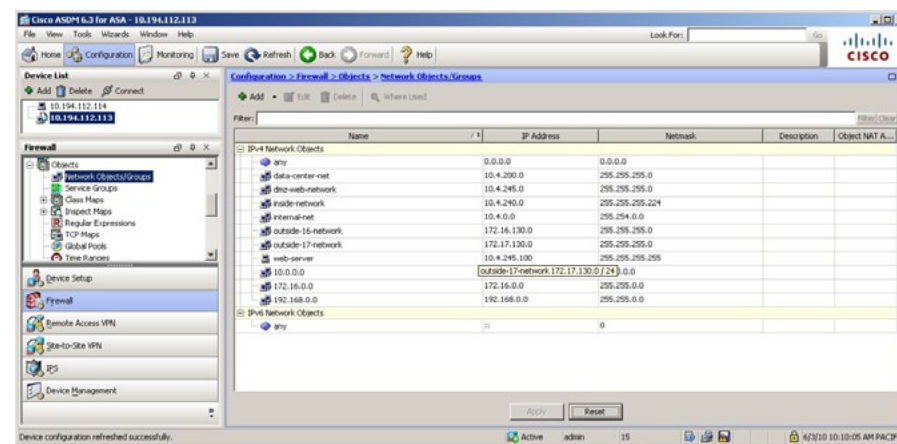
Procedure steps:

1. Configure network names for network hosts and subnets
2. Configure dynamic NAT
3. Define an object-group of hosts that will not be included in the NAT policy
4. Add the NAT Exempt rule, using the exempt hosts' object-group
5. Define static NAT for hosts in the DMZ(s)

Step 1: Navigate to **Configuration > Firewall > Objects > Network Objects/Groups** and configure intuitive names for network hosts and subnets. These names will be used for NAT configuration, as well as Access-Rule definition. Apply names that will be applicable for all parts of the configuration (Figure 31).

Using address-family names and object-groups improves ASDM and command-line usability for the Cisco ASA, as the various IP networks and hosts within the network are represented as names instead of IP addresses. Since the SBA for Large Agencies—Borderless Networks encompasses the 10.4.0.0 and 10.5.0.0 networks, the entire inside network can be represented by the 10.4.0.0/15 subnet.

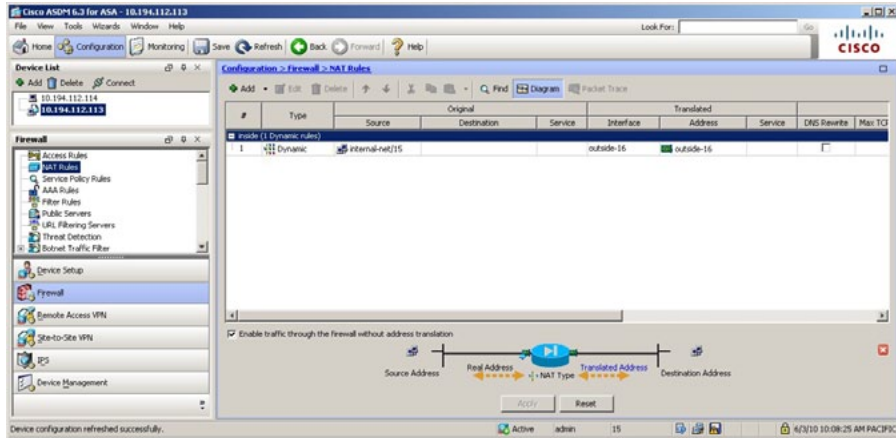
Figure 31. Configure Network Object Names



Step 2: Configure the Dynamic NAT rule that will be used for the inside network in **Configuration > Firewall > NAT Rules** (Figure 32).

An Internet Edge 5K configuration that uses only one outside interface will have one 'global' configuration line.

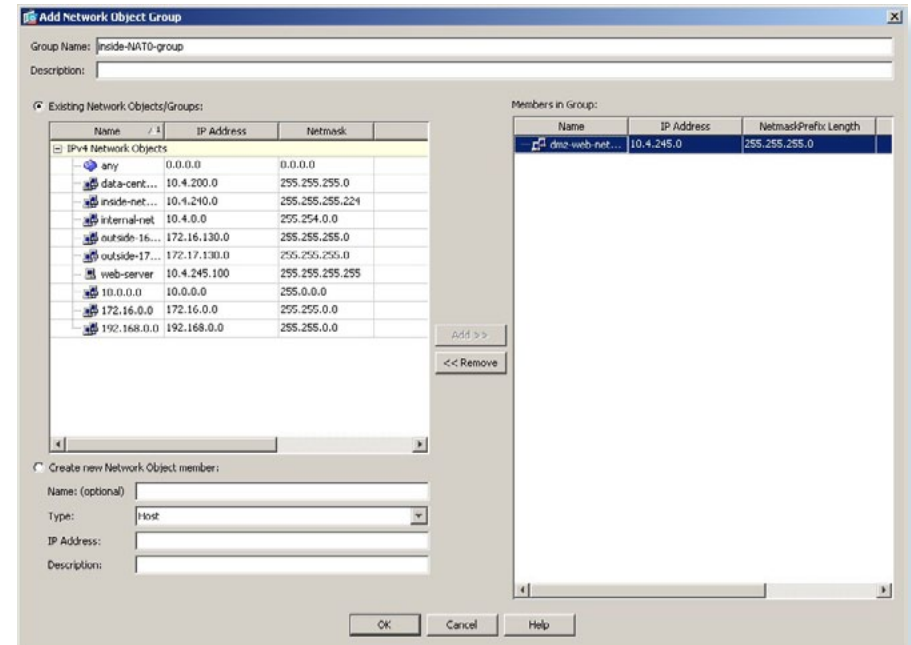
Figure 32. Define Dynamic NAT for Internet Edge 5K



Step 3: Add a network object-group for NAT exemption in the **Configuration > Firewall > Objects > Network Objects/Groups** panel (Figure 33).

The NAT exemption object-group acts as a container for all of the subnets that should be exempt from outbound NAT when the firewall carries traffic to and from the 'inside' network and the DMZ. Using a network object-group provides more flexibility if you add multiple DMZs and remote-access pools that will be exempted from NAT.

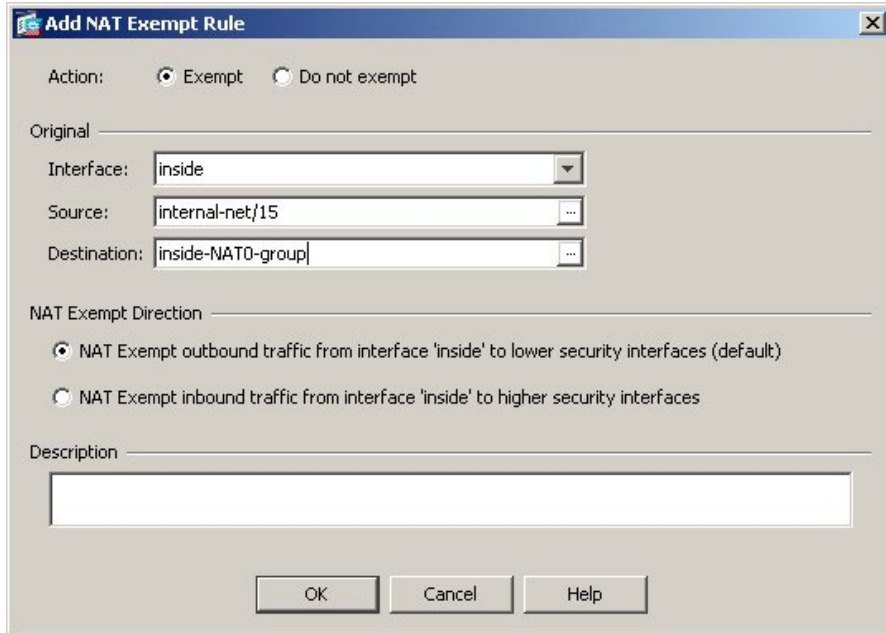
Figure 33. Define Inside NAT0 Network Object-Group



Step 4: Define the Inside NAT Exempt rule in the **Configuration > Firewall > NAT Rules** panel (Figure 34).

This rule uses the object-group from the previous step to the inside-network source address range.

Figure 34. Define Inside NAT Exemption Rule

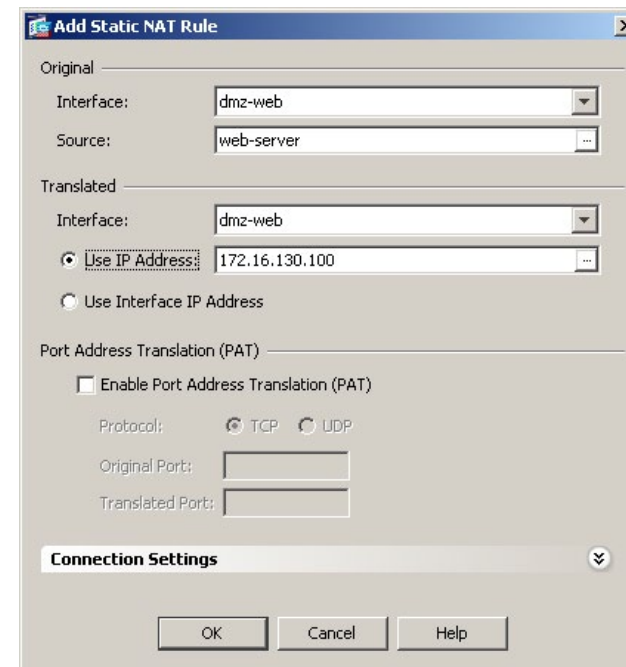


The 'Add NAT Exempt Rule' dialog box is shown. It has a title bar with a close button. The 'Action' section has two radio buttons: 'Exempt' (selected) and 'Do not exempt'. The 'Original' section has three fields: 'Interface' (dropdown menu showing 'inside'), 'Source' (text field with 'internal-net/15' and a browse button), and 'Destination' (text field with 'inside-NAT0-group' and a browse button). The 'NAT Exempt Direction' section has two radio buttons: 'NAT Exempt outbound traffic from interface 'inside' to lower security interfaces (default)' (selected) and 'NAT Exempt inbound traffic from interface 'inside' to higher security interfaces'. The 'Description' section has a large text area. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Step 5: Define static translation policies for Internet traffic to and from the DMZs (Figure 35).

All servers that are exposed to the Internet require a static translation. This configuration is also applied in **Configuration > Firewall > NAT Rules**.

Figure 35. Define Internet Edge 5K Static Translations for DMZ Hosts



The 'Add Static NAT Rule' dialog box is shown. It has a title bar with a close button. The 'Original' section has two fields: 'Interface' (dropdown menu showing 'dmz-web') and 'Source' (text field with 'web-server' and a browse button). The 'Translated' section has two fields: 'Interface' (dropdown menu showing 'dmz-web') and 'Use IP Address' (radio button, selected) with a text field containing '172.16.130.100'. There is also a 'Use Interface IP Address' radio button. The 'Port Address Translation (PAT)' section has a checkbox 'Enable Port Address Translation (PAT)' which is unchecked. Below it are 'Protocol' (radio buttons for 'TCP' and 'UDP', with 'TCP' selected), 'Original Port' (text field), and 'Translated Port' (text field). At the bottom is a 'Connection Settings' section with a dropdown arrow. At the very bottom are 'OK', 'Cancel', and 'Help' buttons.

Executing the preceding steps in ASDM will apply the following CLI configuration:

```
names
name 10.4.0.0 internal-net
access-list INSIDE NAT0 OUTBOUND extended permit ip internal-
net 255.254.0.0 object-group NAT0-DMZ-EXEMPT
global (outside) 1 interface
nat (inside) 0 access-list INSIDE NAT0 OUTBOUND
nat (inside) 1 internal-net 255.254.0.0
```

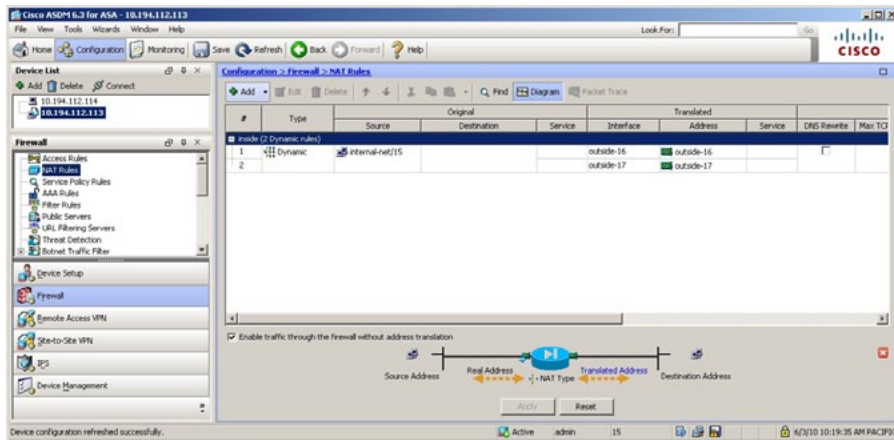
Internet Edge 10K NAT Configuration

The Internet Edge10K design requires additional 'global' NAT configuration for the second outside interface.

Step 1: Configure both interfaces that will be used for the outside (global) addresses (Figure 36).

An Internet Edge10K configuration that uses two outside interface will need two 'global' configuration lines, one for each outside interface.

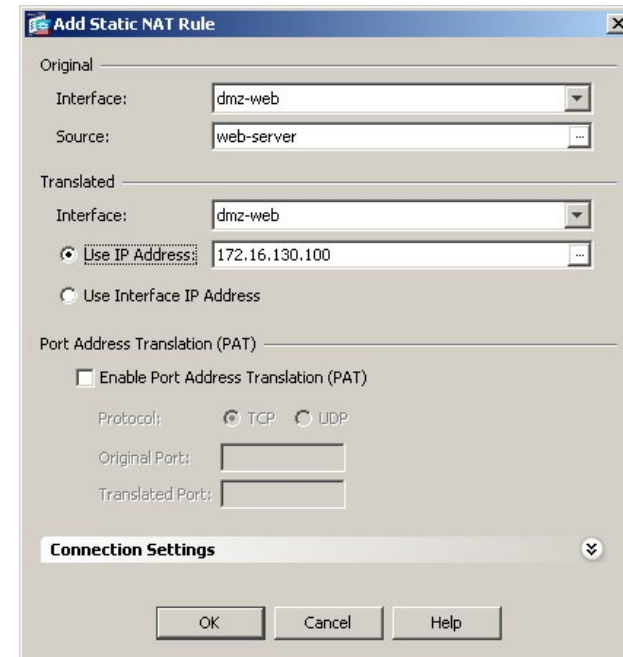
Figure 36. Define Dynamic NAT for Internet Edge-10K



Step 2: Define additional translation rules for traffic to and from the DMZs (Figure 37).

NOTE: Any host that should be accessible from the primary or secondary ISP connections must have a static translation for both outside interfaces. This configuration, shown here for completeness, is more applicable to offering a secondary address for hosts such as email servers or a secondary site-to-site VPN hub.

Figure 37. Define Internet Edge 10K Static Translations for DMZ Hosts



Executing the preceding steps in ASDM will apply the following CLI configuration:

```
global (outside-16) 1 interface
global (outside-17) 1 interface
nat (inside) 0 access-list INSIDE NAT0 OUTBOUND
nat (inside) 1 internal-net 255.254.0.0
```

Firewall Policy Development and Configuration

An agency should have an IT security policy to use as a reference for defining its firewall policy. If there is no documented security policy, it is very difficult to create a firewall policy for the agency because no consistent set of rules can be enforced.

Policy Recommendations

Network security policies can be broken down into two basic categories: ‘whitelist’ policies and ‘blacklist’ policies. A whitelist-based policy offers a stronger initial security posture because all traffic is blocked except for applications that are explicitly allowed. However, whitelist policies are more likely to interfere with network applications and are more difficult to maintain as each new application must be permitted through the firewall. A whitelist policy is easily recognized because the last access control entry (ACE) denies all traffic (i.e., deny ip any any). Whitelist policies are best suited for traffic from the Internet to services in the DMZ.

Information needed to be able to effectively define a whitelist security policy
What applications will be used on the network? Can their traffic be characterized at the protocol level?
Is a detailed description of application behavior available to facilitate troubleshooting if the security policy interferes with the application?

A blacklist policy is generally more suitable for requests from the ‘inside’ network to the Internet. This type of policy offers reduced operational burden and minimizes the likelihood that the security policy will interfere with Internet applications. Blacklist policies are the opposite of whitelist policies, they only stop traffic that is explicitly denied, typically applications are not allowed because of an agency’s policy or because they expose the agency to malicious traffic. A blacklist policy is recognizable by the last ACE if the rule set permits all traffic that has not already been denied (that is, “permit ip any any”).

In some cases, traffic (such as web content) of high operational value is very difficult to distinguish from traffic with no operational value, such as malware and entertainment traffic. As an adjunct to the Cisco ASA, the Cisco Web Security Appliance offers web filtering for traffic that contains malware or negatively affects user productivity. Additionally, Cisco IPS can be used to block malicious traffic embedded within permitted applications. Cisco WSA and IPS concepts and configuration are discussed in the IPS and Web Security modules in this document.

This document describes whitelist policies to allow traffic from the Internet to the DMZs, and a blacklist policy for traffic from the ‘inside’ destined for the Internet.

Procedure 8 Blacklist Security Policy Configuration

This policy is typically configured so that inside network access to the Internet is blocked only for high-risk services; all other access is allowed.

Blacklist Security Policy Configuration

This policy allows wide-open access from the internal network to the Internet, except for a few specific example services that are blocked.

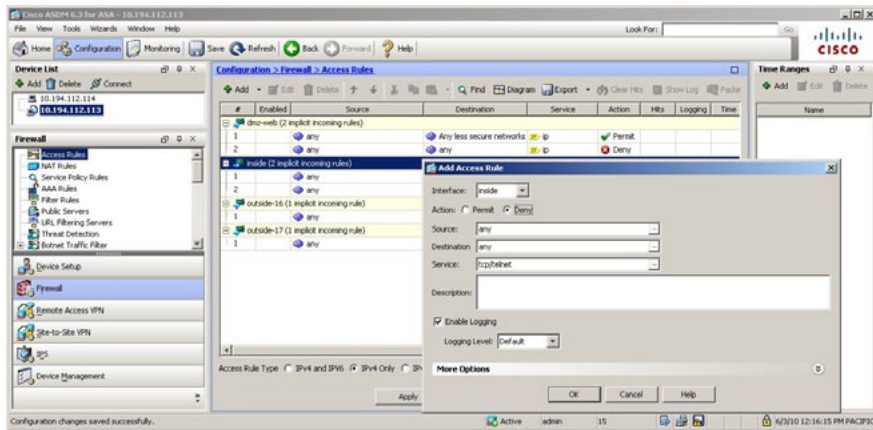
Procedure steps:

- 1. Define a rule blocking telnet access. .
- 2. Add a rule to permit any traffic that is not specifically denied.

Step 1: Define a rule to deny the internal network from sending outbound telnet requests, as well as any other services that must not be allowed past the firewall. (Figure 38).

Telnet is an example of a network service that carries all of its data unencrypted. This poses a risk because hosts that can intercept the data can potentially view sensitive data. For this reason outbound telnet is blocked.

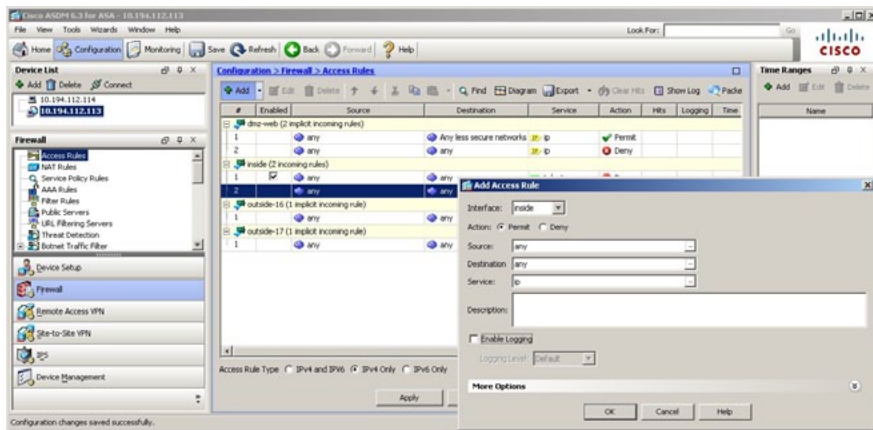
Figure 38. In the Firewall > Access Rules panel, configure Rule to Block Telnet



Step 2: Add a rule to allow all remaining traffic that has not been specifically blocked or allowed (Figure 39).

This final rule realizes the 'blacklist' policy described above; all traffic that is not explicitly denied is permitted. The 'allow any any' rule must be added before the implicit 'deny any any' rule at the end of all Cisco ASA access rule sets. Disable logging on this rule, unless logging is needed for debugging.

Figure 39. Add 'allow any any' Rule



Executing the preceding steps in ASDM will apply the following CLI configuration:

```
access-list INSIDE_ACCESS_IN extended deny tcp internal-net
255.254.0.0 any eq telnet
access-list INSIDE_ACCESS_IN extended permit tcp internal-net
255.254.0.0 dmz-mail-net 255.255.255.0 eq smtp
access-list INSIDE_ACCESS_IN extended deny tcp internal-net
255.254.0.0 any eq smtp
access-list INSIDE_ACCESS_IN extended permit ip internal-net
255.254.0.0 any
access-group INSIDE_ACCESS_IN in interface inside
```

Procedure 9 Whitelist Security Policy Configuration

A whitelist policy allows access from the Internet to a web server in the DMZ..

Procedure steps:

1. Define a firewall policy to allow connections to HTTP and HTTPS from the Internet to a specific server.

Web DMZ Policy Configuration

The Web DMZ offers HTTP and HTTPS service for the Internet. This could provide capabilities to support employee/partner web-portal access, basic customer service and support, small-scale eCommerce or B2B service, or other appropriate tasks.

Step 1: Define an access-control entry to allow HTTP and HTTPS access to the web Server (Figure 40).

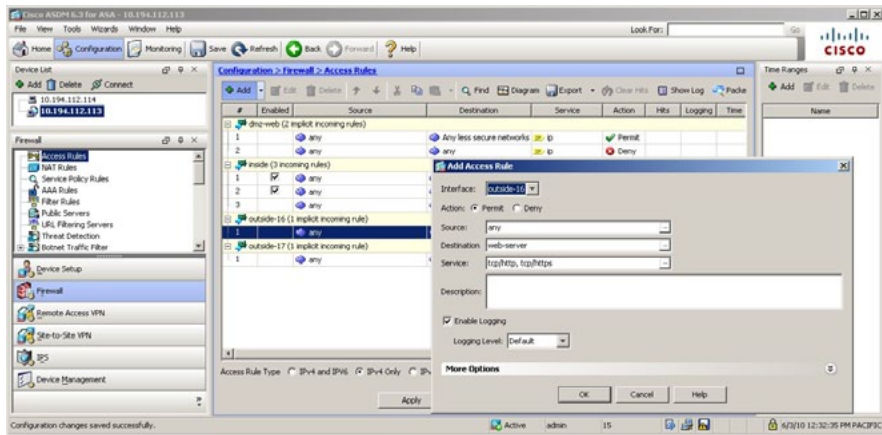
This policy is applied on the outside-interface Access Rule. This design offers no description to open access from the Web DMZ to the internal network, as this poses a substantial security risk.



Tech Tip

Each security policy is unique to the policy and management requirements of an agency. Examples in this document are intended to illustrate policy configuration concepts.

Figure 40. Define Inbound Web DMZ Policy



Executing the preceding steps in ASDM will apply the following CLI configuration:

```
access-list OUT-ACCESS-IN extended permit tcp any dmz-web-net
255.255.255.0 eq https
access-list OUT-ACCESS-IN extended permit tcp any dmz-web-net
255.255.255.0 eq www
access-group OUT-ACCESS-IN in interface outside-16
access-list DMZ-MAIL ACCESS IN extended permit tcp dmz-mail-
net 255.255.255.0 host inside-mail eq 25
access-list DMZ-MAIL ACCESS IN extended permit object-group
TCPUDP dmz-mail-net 255.255.255.0 host dns-server eq domain
access-list DMZ-MAIL ACCESS IN extended permit tcp dmz-mail-
net 255.255.255.0 internal-lan 255.255.255.0
access-group DMZ-MAIL-ACCESS_IN in interface dmz-mail
access-list OUT-ACCESS-IN extended permit tcp any host outside-
mail-1 eq smtp
access-list OUT-ACCESS-IN extended permit tcp any dmz-web-net
255.255.255.0 eq https
access-list OUT-ACCESS-IN extended permit tcp any dmz-web-net
255.255.255.0 eq www
access-group OUT-ACCESS-IN in interface outside-16
```

Whitelist Security Policy Development and Troubleshooting

Whitelist policy development can be challenging. If identifying all applications that must be permitted through the firewall is difficult, enable logging for all traffic that is handled by the 'deny' action at the end of the rule set. This will offer visibility for traffic that is not specifically allowed and needs an explicit firewall rule. Logs will indicate application activity and illustrate the specific rules required to enable applications' requirements.

Verify Firewall Policy

Test the Cisco ASA configuration to verify that the policy behaves as expected.

Firewall High Availability

The Cisco ASAs are set up as a highly available active/standby pair. Active/standby is used, rather than an active/active configuration, because this is a more common configuration and allows the same appliance to be used for firewall and VPN services (VPN functionality is disabled on the ASA in active/active). In the event that the active ASA appliance fails or needs to be taken out of service for maintenance, the secondary ASA appliance will assume all active firewall, IPS, and VPN functions. In an active/standby configuration, only one device is passing traffic at a time; thus, the Cisco ASAs must be sized so that the entire traffic load can be handled by either device in the pair.

Both units in the failover pair must be the same model, with identical feature licenses and Security Services Modules (SSMs) (if SSMs are installed). The secondary ASA unit needs to be powered up and cabled to the same networks as the primary for failover to be enabled.

One interface on each ASA is configured as the state-synchronization interface, which the ASAs use to share configuration updates, determine which device in the high-availability (HA) pair is active, and exchange state information for active connections. The failover interface carries the state synchronization information. All session state is replicated from the primary to the standby unit through this interface. There can be a substantial amount of data, and it is recommended that this be a dedicated interface.

In this example, GigabitEthernet 0/2 is the failover interface. A crossover cable connects these ports on the primary and secondary appliances.

Procedure 10 HA Configuration

Configure active-standby failover.

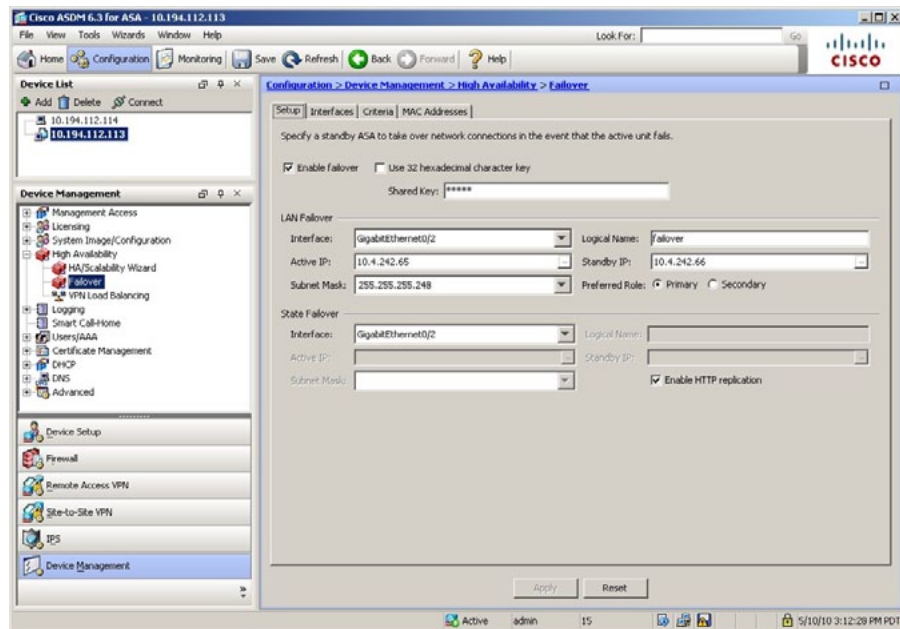
Procedure steps:

1. Enable failover and define primary unit and failover interface
2. Define monitored interfaces' standby addresses
3. Adjust failover timers
4. Apply standby configuration to secondary unit.
5. Verify failover sync

Step 1: Browse to the 'Setup' panel on **Device Management > High Availability > Failover**; enable failover, define which appliance will be the primary unit, and set the failover interface (Figure 41).

The "failover key" value must match on both devices in an active-standby pair. This key is used for two purposes; to authenticate the two devices to each other, and to secure state synchronization messages between the devices that enable the ASA pair to maintain service for existing connections in the event of a failover.

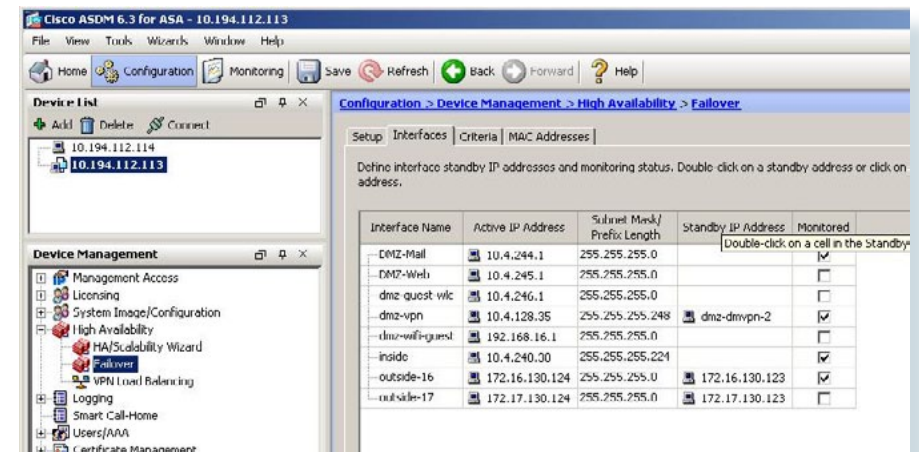
Figure 41. Define Failover Configuration



Step 2: On the 'Interfaces' panel on **Device Management > High Availability > Failover**, define interfaces' standby addresses (Figure 42).

All of the devices' interfaces that are included in the failover configuration have two IP addresses assigned: a primary, active IP address; and a standby IP address. When the appliances swap roles (standby becomes active, or vice versa), the addresses swap between the active and standby interfaces. The standby address must be configured in the same IP subnet as the active address, as the devices pass traffic between each other to monitor interface state. If an interface connects to a network that does not require high availability, then no standby address is needed; however, this design offers HA for all networks on the firewall, thus, all of the appliances' interfaces have addresses defined for the 'active' and 'standby' devices.

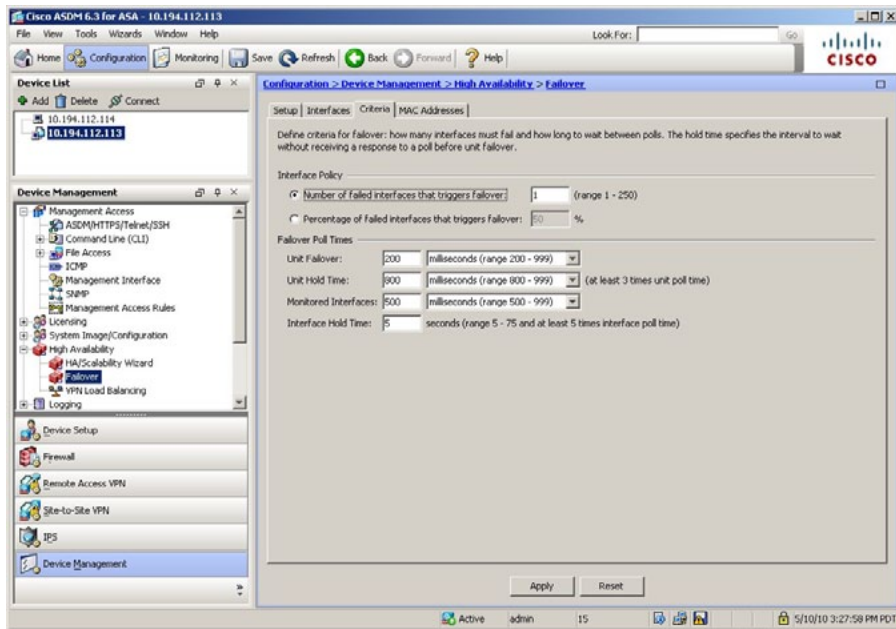
Figure 42. Define Interface Standby Addresses



Step 3: On the 'Criteria' panel on **Device Management > High Availability > Failover**, adjust the failover times to offer a shorter high-availability failover interval (Figure 43).

By default, the ASA can take from 2 to 25 seconds to recover from a failure. Tuning the failover poll times can reduce that to 0.5 to 5 seconds. On an appropriately sized ASA, the poll times can be tuned down without performance impact to the ASA, which minimizes the downtime a user experiences during failover. The configuration lines that begin with "failover polltime" reduce the failover timers from the defaults to achieve sub-second failover. Reducing the failover timer intervals below these values is not recommended.

Figure 43. Adjust Failover Timers



Executing the preceding steps in ASDM will apply the following CLI configuration to the primary Cisco ASA:

```
failover
failover lan unit primary
failover lan interface failover GigabitEthernet0/2
failover key [key]
failover replication http
failover link failover GigabitEthernet0/2
failover interface ip failover 10.4.242.65 255.255.255.248
standby 10.4.242.66
interface GigabitEthernet0/0
 ip address [10.4.240.30] [255.255.255.0] standby [10.4.240.29]
failover polltime unit msec 200 holdtime msec 800
failover polltime interface msec 500 holdtime 5
```

Step 4: Apply the secondary ASA HA configuration to the standby peer.

Apply this block of configuration (after customizing for the deployment) using the command-line interface on the Cisco ASA's console port. Remember to issue the 'no shut' command on both devices' failover interface, if the interfaces have not already been enabled:

```
failover
failover lan unit secondary
failover lan interface failover GigabitEthernet0/2
failover polltime unit msec 200 holdtime msec 800
failover polltime interface msec 500 holdtime 5
failover key [key-value]
failover replication http
failover link failover GigabitEthernet0/2
failover interface ip failover 10.4.242.65 255.255.255.248
standby 10.4.242.66
```

Step 5: Verify standby synchronization between the Cisco ASA devices.

Issue the **show failover** command on the ASA's Command-Line Interface.

```
asa5540A# sh failover
Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Unit Poll frequency 200 milliseconds, holdtime 800 milliseconds
Interface Poll frequency 500 milliseconds, holdtime 5 seconds
Interface Policy 1
Monitored Interfaces 5 of 210 maximum
failover replication http
Version: Ours 8.2(2), Mate 8.2(2)
Last Failover at: 17:07:53 PACIFIC May 27 2010
  This host: Primary - Active
    Active time: 57475 (sec)
    [output deleted]
  Other host: Secondary - Standby Ready
    [output deleted]
```

Firewall Summary

This section has described concepts and configuration for routing to the Internet, firewall management and monitoring, and inside-network and DMZ connectivity and routing. NAT and firewall policy recommendations and configuration for the private LAN, various service networks, and the wireless guest network were also covered. The section finished with a discussion and configuration of active-standby failover for Cisco ASA firewalls.

Notes

Intrusion Prevention

Agency Overview

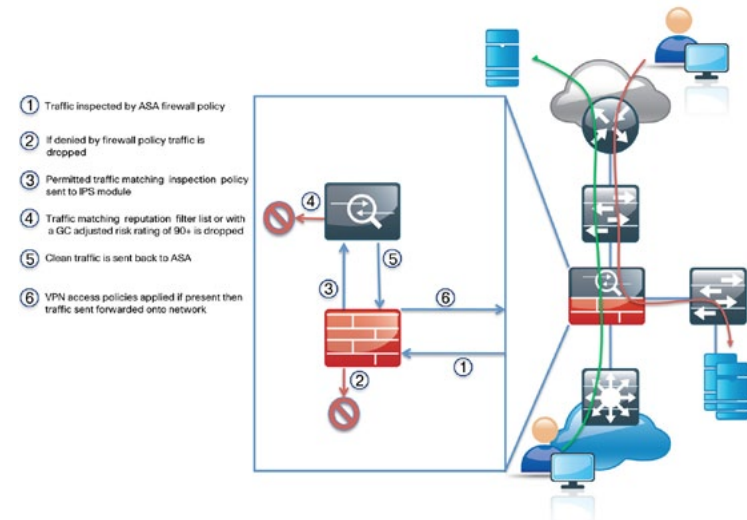
Internet services have become a key part of day-to-day operations for many agencies today. Providing secure Internet access, while preventing malicious content from entering an agency is critical to maintaining employee productivity. In addition to client access to the Internet, agencies have near universal need to have a web presence up and available for partners and clients to access basic information about the agency. When you place agency information on the Internet, you run a risk of exposure of data through an attack on the public-facing services. For an agency to use the Internet effectively, solutions must be found for all of these concerns.

Technical Overview

Worms, viruses, and botnets pose a substantial threat to agencies. To minimize the impact of network intrusions, intrusion prevention systems (IPSs) and intrusion detection systems (IDSs) can be deployed to provide additional protection for the traffic that is permitted through the Internet edge firewall. IPS is a complementary technology to the firewall and inspect traffic that is permitted by the firewall policy for attacks. If an IPS detects an attack, the offending traffic is dropped and an alert is sent. The IPS Security Service Module (SSM) can also run in an IDS mode where attacks are detected and alerted, but not dropped. Deploying the SSM in IDS mode can be helpful when initially deploying IPS to make sure that no production traffic is affected.

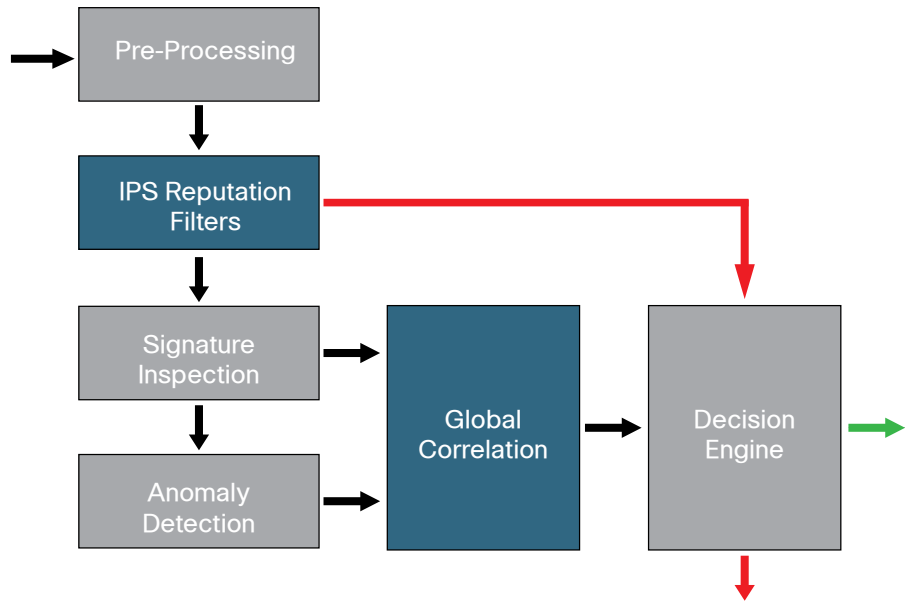
This design employs the Cisco Adaptive Inspection Prevention Security Service Module (AIP-SSM) for IPS services in the Internet edge Cisco ASA 5500 series firewalls. The design offers several options that are based on the performance requirements of the agency. For the Internet Edge 5K, the ASA 5520 with AIP-SSM-20 is recommended. The SSM-20 supports up to 375 Mbps of traffic for IPS inspection. For larger networks, like the Internet Edge 10K design, the ASA 5540 with AIP-SSM-40 will support up to 650 Mbps of traffic for IPS inspection. It is important to remember that the Internet edge firewall and IPS have more than just employee Internet traffic going through the box. Internal traffic to servers in the DMZ, wireless guest traffic, site-to-site VPN, and remote access VPN traffic all combine to make the throughput requirements for the Internet edge firewall and IPS much higher than Internet connection speed.

Figure 44. Packet Flow Through an ASA/AIP-SSM



IPS modules integrated into the ASA rely on the ASA for high availability services. The ASAs in the Internet edge are deployed in an active/standby configuration, if the primary ASA fails, then the secondary ASA will take over all firewall operations and the traffic will be inspected by the IPS module in the secondary ASA.

Figure 45. IPS Processing Flowchart



Cisco IPS version 7.0 added a set of features that allow the system to make informed decisions on whether to permit or block traffic based off of reputation. Cisco uses reputation in two key ways on the IPS:

- Reputation filters: a small list of IP addresses that have been hijacked or are owned by malicious groups
- Global Correlation Inspection: a rating system for IP address based off of prior behavior.

Reputation filters allow the IPS to block all traffic from known bad addresses before any significant inspection is done (Figure 45). Global Correlation uses the reputation of the attacker in conjunction with the risk rating associated with the signature that triggered to come up with a new risk rating and drop traffic that is more likely to be malicious (Figure 46).

Figure 46. Reputation Effect on Risk Rating

Reputation Effect on Risk Rating		Reputation of Attacker																			
		Standard Mode										Reputation of Attacker									
		Blue Deny Packet										Red Deny Attacker									
		-0.5	-1	-1.5	-2	-2.5	-3	-3.5	-4	-4.5	-5	-5.5	-6	-6.5	-7	-7.5	-8	-8.5	-9	-9.5	-10
Initial Risk Rating	80	80	80	84	87	90	92	94	95	97	98	99	99	100	100	100	100	100	100	100	
	81	81	81	84	87	90	92	94	96	97	98	99	100	100	100	100	100	100	100	100	
	82	82	82	85	88	91	93	95	96	97	98	99	100	100	100	100	100	100	100	100	
	83	83	83	85	88	91	93	95	96	98	99	99	100	100	100	100	100	100	100	100	
	84	84	84	86	89	92	94	95	97	98	99	100	100	100	100	100	100	100	100	100	
	85	85	85	87	90	92	94	96	97	98	99	100	100	100	100	100	100	100	100	100	
	86	86	86	87	90	92	94	96	97	98	99	100	100	100	100	100	100	100	100	100	
	87	87	87	88	91	93	95	96	98	99	100	100	100	100	100	100	100	100	100	100	
	88	88	88	88	91	93	95	97	98	99	100	100	100	100	100	100	100	100	100	100	
	89	89	89	89	92	94	96	97	98	99	100	100	100	100	100	100	100	100	100	100	
	90	90	90	90	92	94	96	97	99	100	100	100	100	100	100	100	100	100	100	100	
	91	91	91	91	93	95	97	98	99	100	100	100	100	100	100	100	100	100	100	100	
	92	92	92	92	93	95	97	98	99	100	100	100	100	100	100	100	100	100	100	100	
	93	93	93	93	94	96	97	99	100	100	100	100	100	100	100	100	100	100	100	100	
	94	94	94	94	95	96	98	99	100	100	100	100	100	100	100	100	100	100	100	100	
	95	95	95	95	95	97	98	99	100	100	100	100	100	100	100	100	100	100	100	100	
	96	96	96	96	96	97	99	100	100	100	100	100	100	100	100	100	100	100	100	100	
	97	97	97	97	97	98	99	100	100	100	100	100	100	100	100	100	100	100	100	100	
	98	98	98	98	98	99	100	100	100	100	100	100	100	100	100	100	100	100	100	100	
	99	99	99	99	99	99	100	100	100	100	100	100	100	100	100	100	100	100	100	100	
	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	

A discussion about how traffic moves through the ASA/AIP-SSM combination can be found here:

http://www.cisco.com/en/US/partner/docs/security/asdm/6_1/user/guide/ips.html#wp1535290

Configuration Details

The first step used to configure an IPS SSM is to session into the module from the ASA and set up basic networking such as IP address, gateway, and access lists to allow remote access to the GUI. Once the basic setup is complete, configuration is easy through a GUI such as IPS Device Manager launched from the ASA Security Device Manager (ASDM) or the IPS Manager Express (IME).

Process

1. Initial Setup
2. IPS Policy
3. IDS Policy

Procedure 1 Initial Setup

Procedure Steps:

1. Session into the module from the ASA
2. Run Setup
3. Configuring the second module
4. Connect to the sensor in ASDM
5. Running the startup wizard
6. Startup Wizard-Sensor Setup

Step 1: Session into the module from the ASA.

After logging into the ASA, the SSM module can be accessed by issuing the following command.

```
ASA5540# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

The default username and password for the IPS module is cisco/cisco. If this is the first time the sensor has been logged into, there will be a prompt to change the password. Change the password to a value that complies with the security policy of the agency.

```
login: cisco Password:
```

NOTICE

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: <http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

Step 2: Run Setup.

After login, run the **setup** command to launch the initial configuration dialog. (In this example, user data is shown in bold.)

```
sensor# setup
    --- Basic Setup ---
    --- System Configuration Dialog ---
```

At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

```
Current time: Mon Apr 19 17:52:08 2010
Setup Configuration last modified: Mon Apr 19 17:51:48 2010
Enter host name[sensor]: SSM-40-A
Enter IP interface[192.168.1.2/24,192.168.1.1]:
10.4.240.27/24,10.4.240.1
Modify current access list?[no]: yes
Current access list entries:
    No entries
Permit: 10.0.0.0/8
Permit:
Use DNS server for Global Correlation?[no]: yes
    DNS server IP address[]: 10.4.200.10
Use HTTP proxy server for Global Correlation?[no]: yes
    HTTP proxy server IP address[]: 128.107.241.169
    HTTP proxy server port number[]: 80
Modify system clock settings?[no]: Participation in the
SensorBase Network allows Cisco to collect aggregated
statistics about traffic sent to your IPS. SensorBase Network
Participation level?[off]: partial
```

If you agree to participate in the SensorBase Network, Cisco will collect aggregated statistics about traffic sent to your IPS. This includes summary data on the Cisco IPS network traffic properties and how this traffic was handled by the Cisco appliances. We do not collect the data content of traffic or other sensitive business or personal information. All data is aggregated and sent via secure HTTP to the Cisco SensorBase Network servers in periodic intervals. All data shared with Cisco will be anonymous and treated as strictly confidential. The table below describes how the data will be used by Cisco.

Participation Level = "Partial":

- Type of Data: Protocol Attributes (e.g. TCP max segment size and options string)
Purpose: Track potential threats and understand threat exposure
- Type of Data: Attack Type (e.g. Signature Fired and Risk Rating)
Purpose: Used to understand current attacks and attack severity
- Type of Data: Connecting IP Address and port
Purpose: Identifies attack source
- Type of Data: Summary IPS performance (CPU utilization memory usage, inline vs. promiscuous, etc)
Purpose: Tracks product efficacy

Participation Level = "Full" additionally includes:

- Type of Data: Victim IP Address and port
Purpose: Detect threat behavioral patterns

Do you agree to participate in the SensorBase Network?[no]:

yes

The following configuration was entered.

```
service host
network-settings
host-ip 10.4.240.27/27,10.4.240.1
host-name SSM-40-A
telnet-option disabled
access-list 10.0.0.0/8
ftp-timeout 300
no login-banner-text
dns-primary-server enabled
address 10.4.200.10
exit
dns-secondary-server disabled
dns-tertiary-server disabled
http-proxy proxy-server
address
port
exit
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service global-correlation
network-participation partial
```

```
exit
[0] Go to the command prompt without saving this config.
[1] Return to setup without saving this config.
[2] Save this configuration and exit setup.
[3] Continue to Advanced setup.
Enter your selection[3]: 2
```

--- Configuration Saved ---

Complete the advanced setup using CLI or IDM. To use IDM, point your web browser at <https://<sensor-ip-address>>.
sensor#

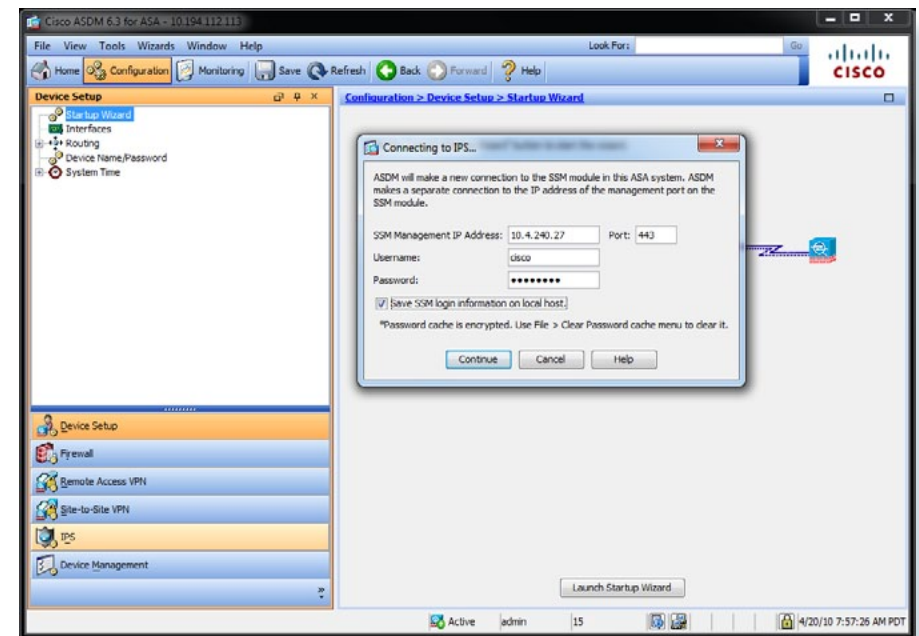
Step 3: Configuring the second module

Press CTRL-X to exit the sensor and drop back into the Cisco ASA command line. To set up the second SSM on the standby ASA, log in to the CLI and rerun the setup script to configure the basic network connectivity. A different hostname must be used on the second SSM so that monitoring systems do not get confused. In the test lab, SSM-40-B was used on the standby SSM.

Step 4: Connect to the sensor in ASDM

At this point the IPS sensors are accessible from ASDM. Log in to ASDM and click on the **Configuration** tab and then click **IPS**. ASDM should display the "Connecting to IPS..." window. Enter the username and password specified on the IPS sensor and click **Continue** (Figure 47).

Figure 47. ASDM Connecting to IPS Module

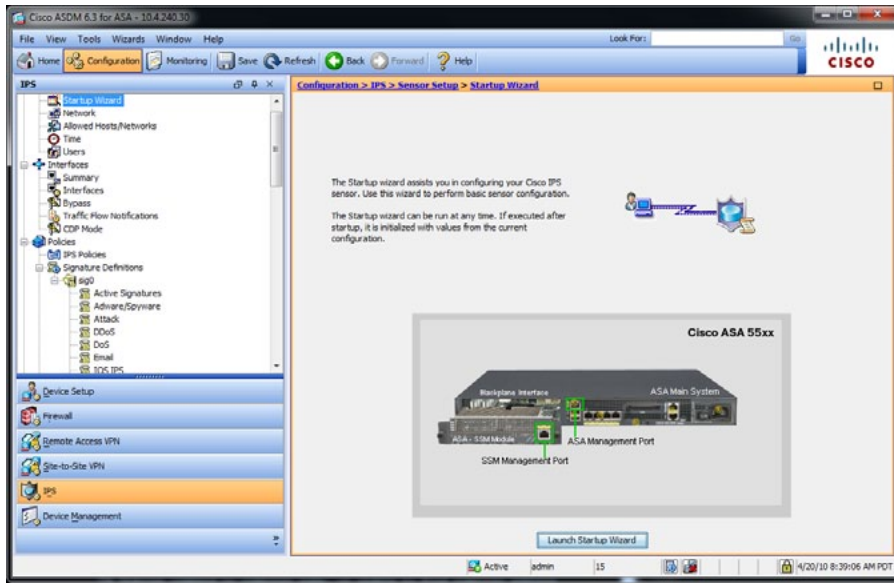


ASDM will import the current configuration from the IPS sensor and the startup wizard launcher will be displayed in the main window.

Step 5: Running the startup wizard

Click **Launch Startup Wizard** (Figure 48).

Figure 48. Startup Wizard

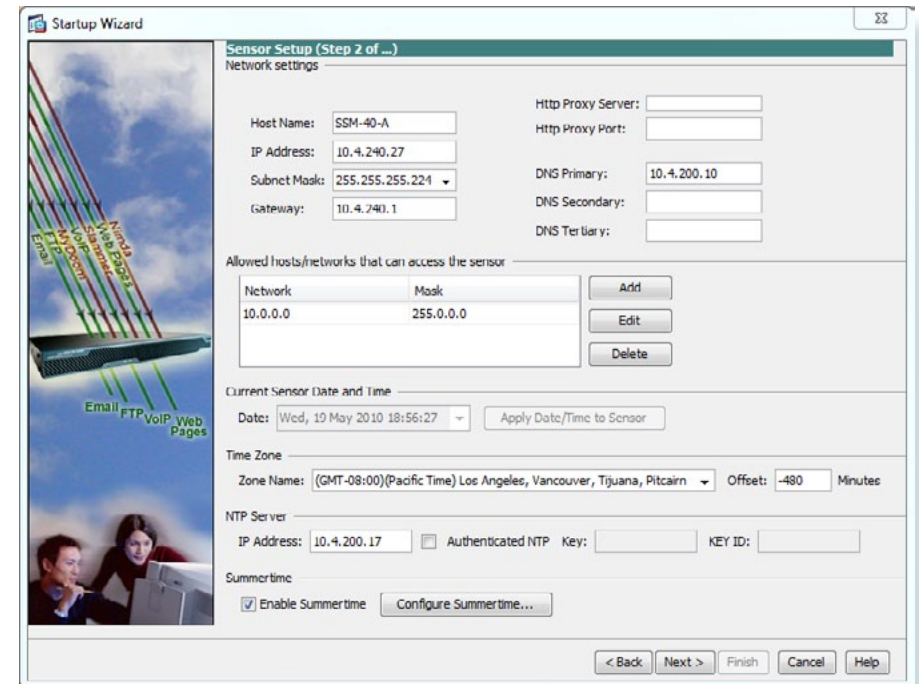


Step 6: Startup Wizard-Sensor Setup

In the Startup Wizard: Sensor Setup, enter an NTP server and any necessary credentials for the server, set the time zone and summertime settings, and add the agency's DNS servers as needed. The Allowed Hosts panel defines which IP addresses the sensor will accept at the management interface (Figure 49).

Click **Next**.

Figure 49. Sensor Setup



IPS Sensor Policy

At this point a decision must be made to run the sensor in IPS mode where the sensor is inline in the traffic path. In this mode the traffic is inspected and can be dropped if it is malicious. The second mode of operation that is available is IDS mode where a copy of the traffic is passively sent to the sensor to be inspected and alerts can be sent if the traffic is malicious. IPS mode provides more protection from Internet threats and has a low risk of blocking important traffic at this point in the network, particularly when it is coupled with reputation-based technologies. IDS mode can be deployed as a temporary solution to see what kind of impact IPS would have on the network and what traffic would be stopped. After the impact is understood and any necessary tuning has been done, then the sensor can be easily changed to IPS mode.

If running the module in IPS (inline) mode, follow procedure 2. If running the module in IDS (promiscuous) mode, follow procedure 3.

Procedure 2 IPS Policy

Procedure 2 Steps:

1. Configuring IPS Policy in Startup Wizard
2. Configuring the IPS Traffic Policy
3. Enabling IPS inspection
4. Edit Virtual Sensor configuration

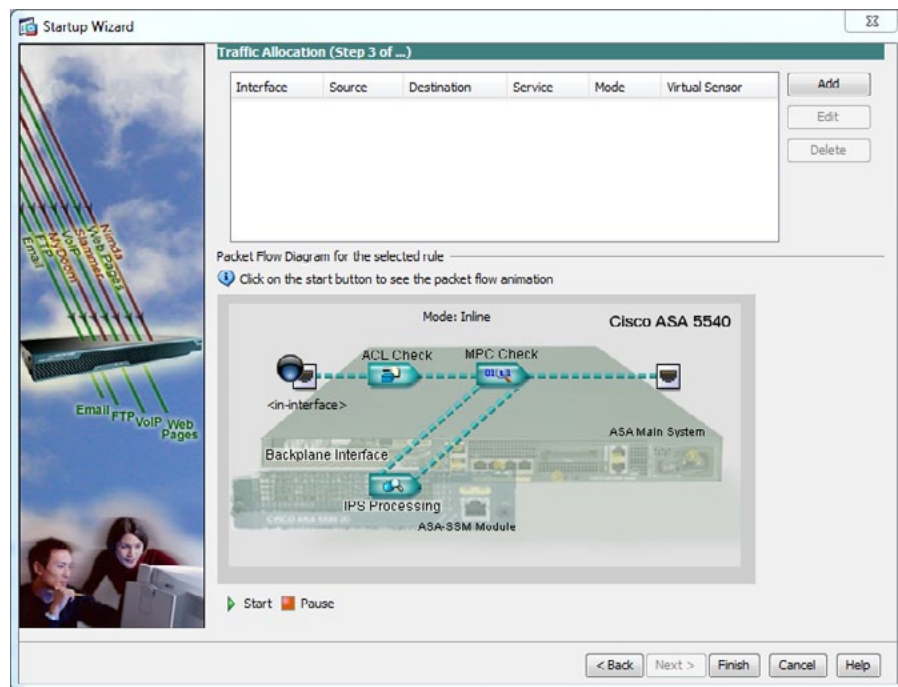
Step 1: Configuring IPS Policy in Startup Wizard

When running the Startup Wizard, the third step is Traffic Allocation where the decision is made of what traffic to send to the IPS module and whether the traffic is sent in inline mode (IPS) or promiscuous mode (IDS).

For IPS mode we will add an inline policy globally that will inspect all traffic in and out of the ASA firewall (Figure 50).

Click **Add**.

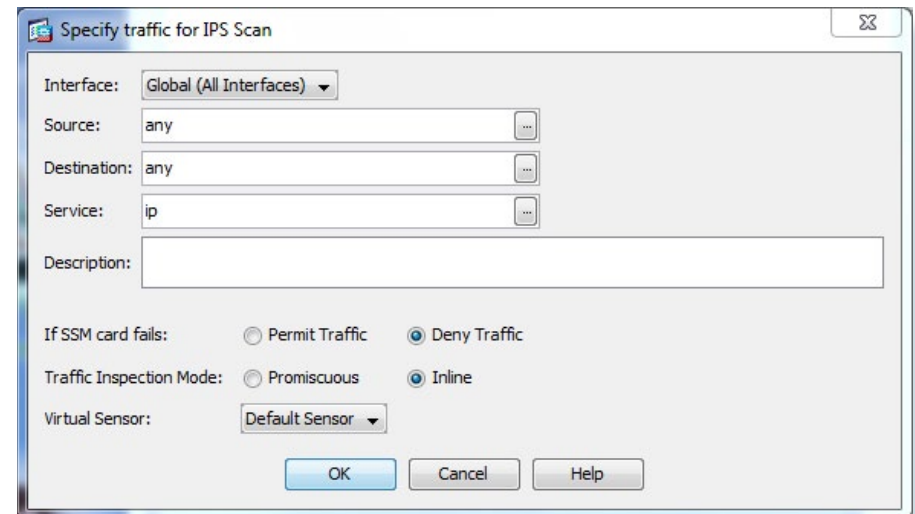
Figure 50. Configuring IPS Policy in ASDM



Step 2: Configuring the IPS Traffic Policy

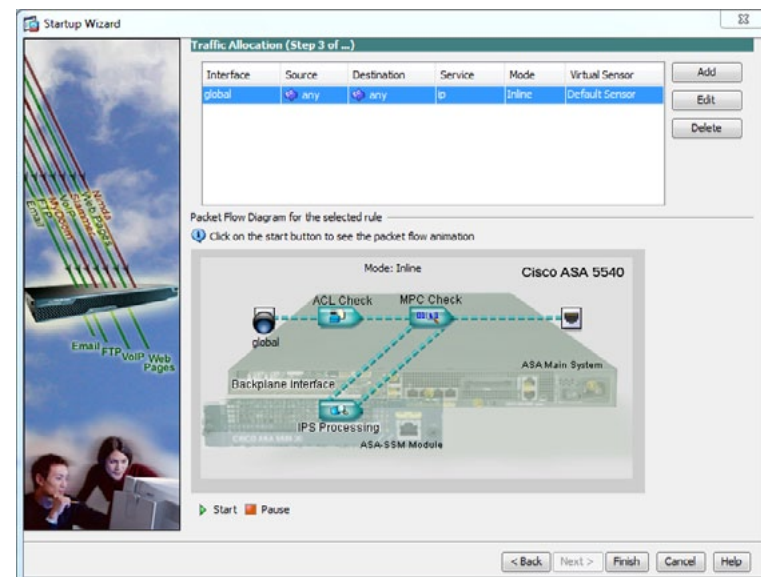
Accept the default settings to inspect all traffic and then click **OK** (Figure 51).

Figure 51. IPS Traffic Policy



A global IPS policy has been configured and is ready to be applied to the sensor. Click **Finish** (Figure 52).

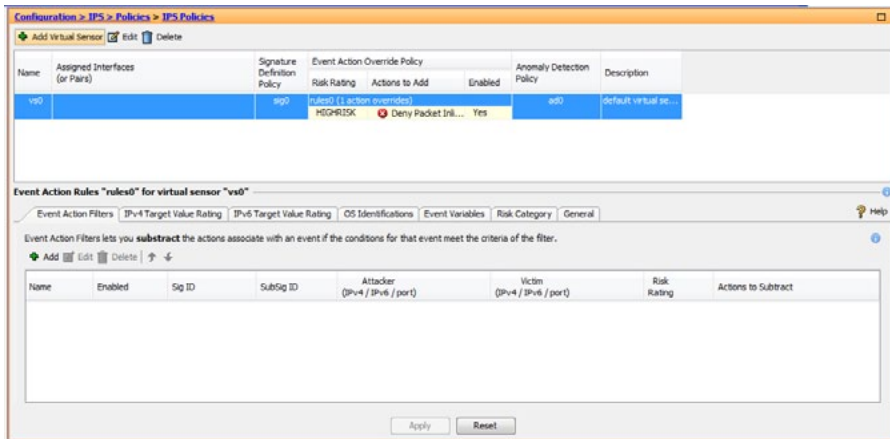
Figure 52. IPS Inline Policy in ASDM



Step 3: Enabling IPS inspection

For the policy to be active on the firewall it must be applied to an interface. Click on **Policies > IPS: Policies** in the lefthand window. Click **Edit** (Figure 53).

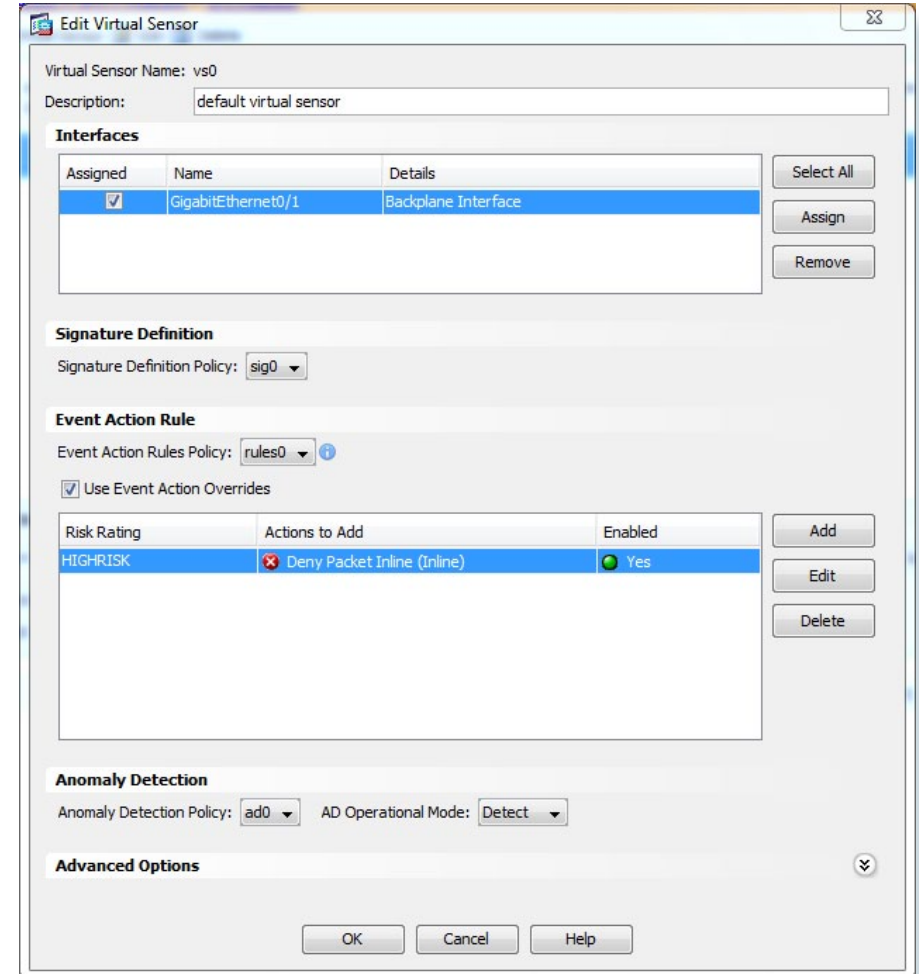
Figure 53. Enabling IPS Inspection



Step 4: Edit Virtual Sensor configuration

Check the box under interfaces and assigned to associate the IPS policy to the ASA's backplane interface. Click **OK** (Figure 54).

Figure 54. Edit IPS Virtual Sensor Configuration



Click **Apply** and save the ASA config to complete the IPS inline setup.

Procedure 3 **IDS Policy**

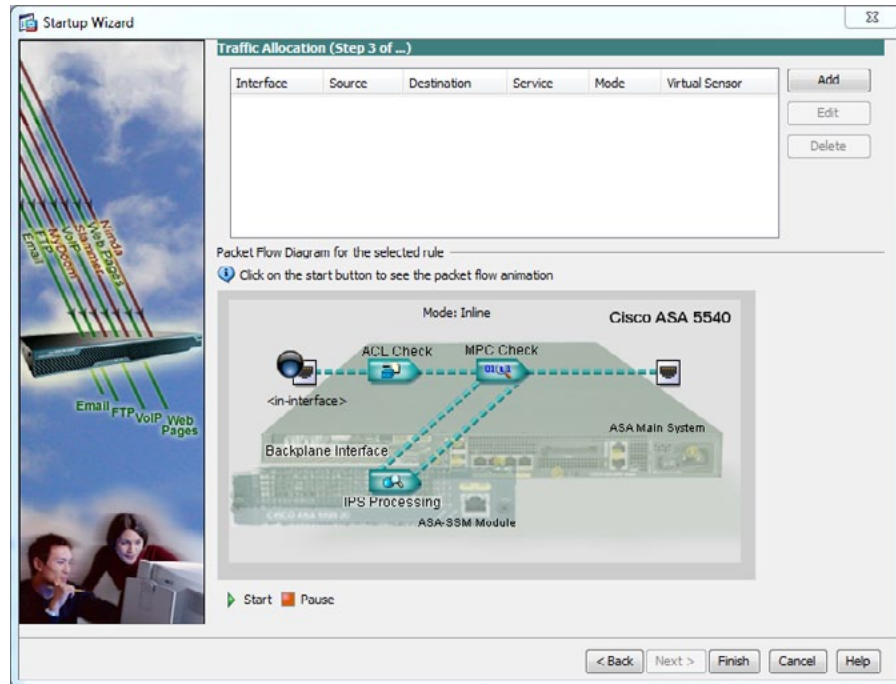
Procedure 3 Steps:

1. Configuring IDS Policy in Startup Wizard
2. Configuring the IDS Traffic Policy
3. Enabling IDS inspection
4. Edit Virtual Sensor configuration

Step 1: Configuring IDS Policy in Startup Wizard

For IDS mode, a promiscuous policy needs to be created in the startup wizard. To add an IDS policy, start by clicking **Add** on screen 3 of the wizard (Figure 55).

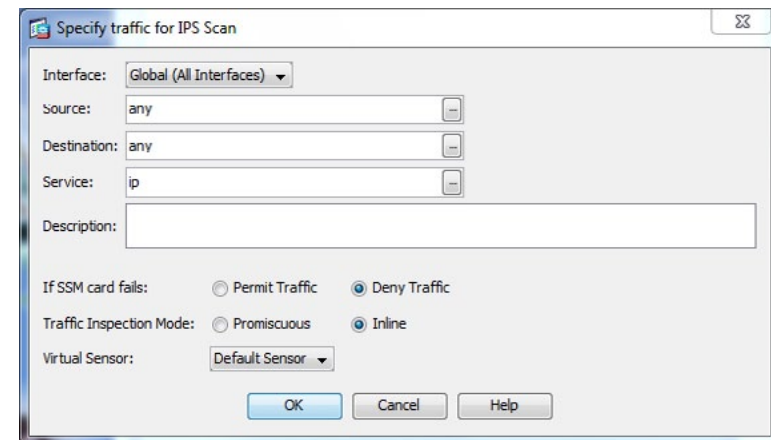
Figure 55. Configuring IDS Policy in ASDM



Step 2: Configuring the IDS Traffic Policy

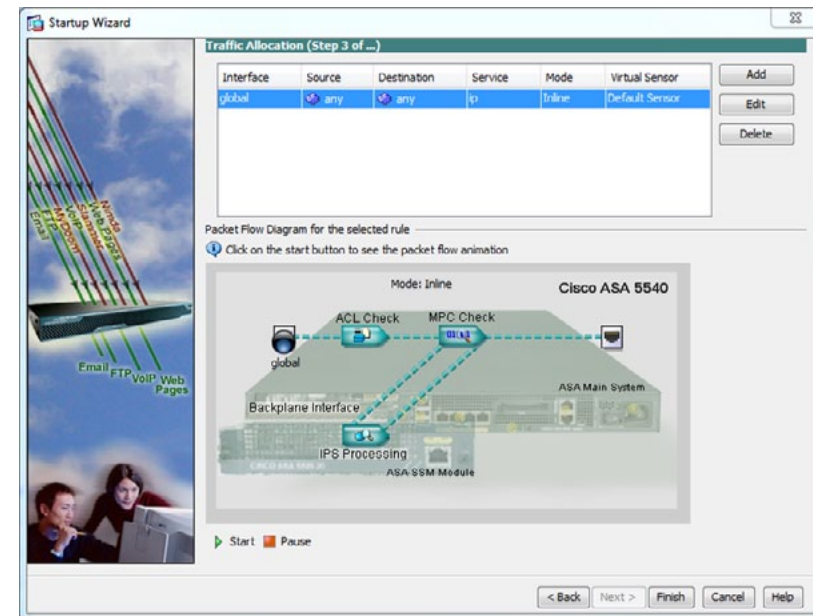
Change the traffic inspection type to Promiscuous and click **OK** (Figure 56).

Figure 56. IDS Traffic Policy



At this point, the promiscuous policy is created and ready to be applied to the sensor. Click **Finish** to complete IDS mode configuration (Figure 57).

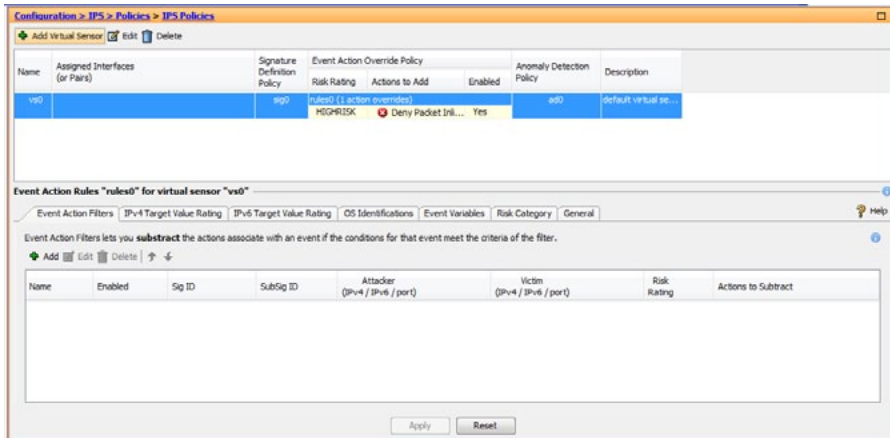
Figure 57. IDS Inline Policy in ASDM



Step 3: Enabling IDS inspection

For the policy to be active on the firewall, it must be applied to an interface. Click on **Policies > IPS > Policies** in the lefthand window. Click **Edit** (Figure 58).

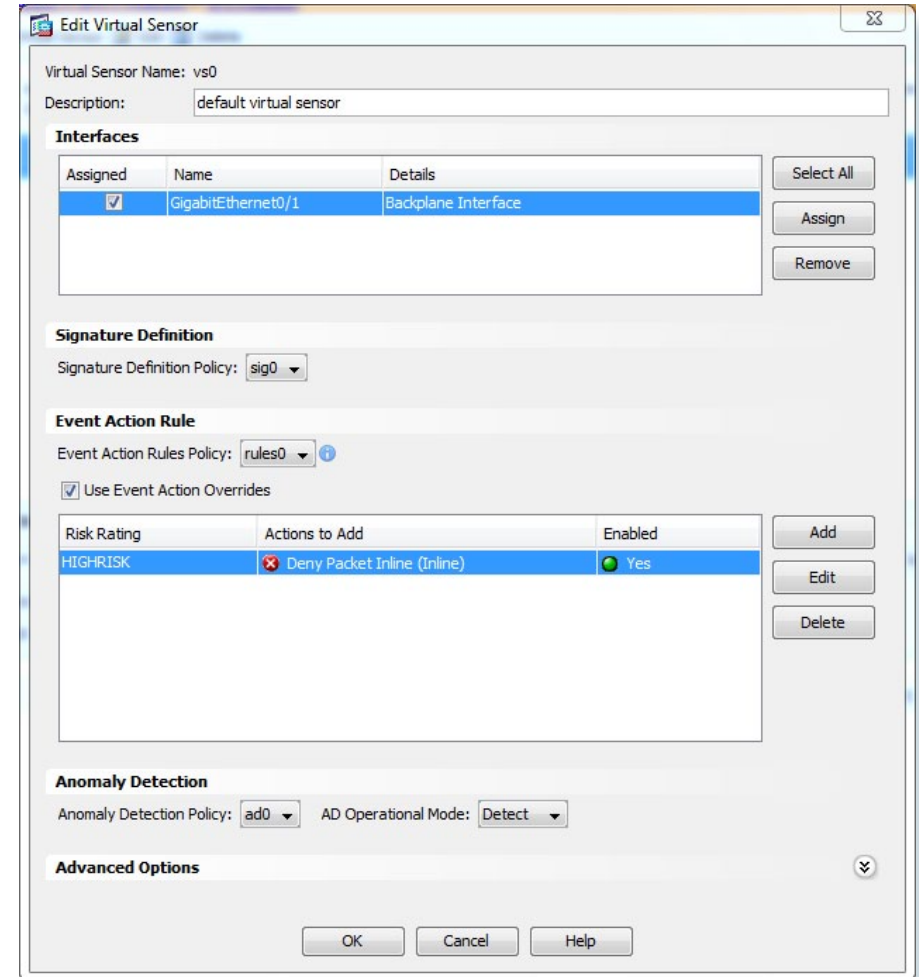
Figure 58. Enabling IDS Inspection



Step 4: Edit Virtual Sensor configuration

Check the box under interfaces and assigned to associate the IPS policy to the ASA's backplane interface. Click **OK** (Figure 59).

Figure 59. Edit IDS Virtual Sensor Configuration

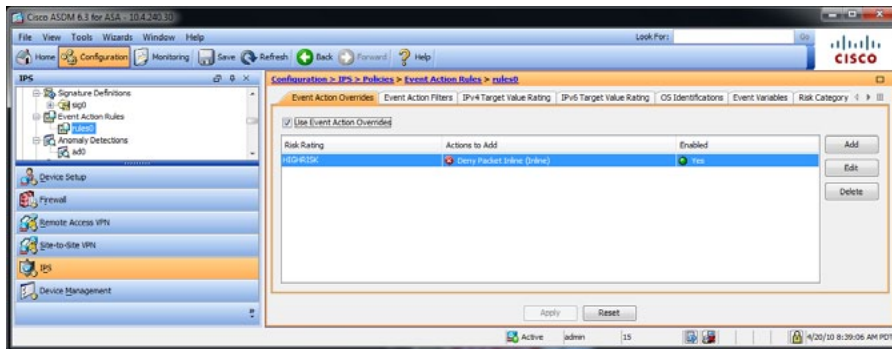


Click **Apply** and save the ASA config to complete the IPS promiscuous setup.

Inline Security Policy Modifications

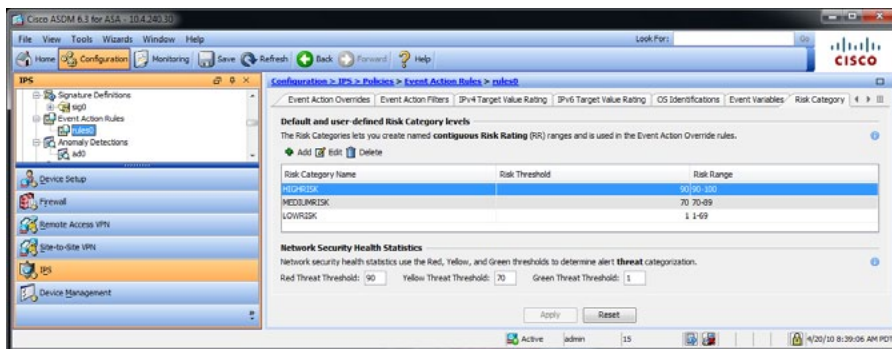
If IPS mode was chosen, the sensor is configured to drop high-risk traffic. This configuration means that if an alert fires with a risk rating of 90, or if the traffic comes from an IP address with a negative reputation that raises the risk rating to 90 or higher, the traffic will be dropped. If the risk rating is raised to 100 because of the source address reputation score, then all traffic from the IP address will be dropped (Figure 60).

Figure 60. IPS Policy



The chances of the IPS dropping traffic that is not malicious with this configuration is very low, but if a more conservative policy is desired, change the HIGHRISK classification from 90-100 to 100-100 by editing the HIGHRISK policy and setting the value to 100 (Figure 61).

Figure 61. IPS Risk Categories



Final Steps

The IPS sensor is now set up and needs to be rebooted for all of the configurations to take effect, if the sensor that is being rebooted is on the primary ASA, the reload will cause a failover to the standby firewall. To check to see if the ASA is the primary firewall, use the **show failover** command to show which ASA is active, log into the ASA that is not the current active box and issue the **failover active** command. Logging back into ASDM should connect to the other ASA (the newly active firewall) with the still unconfigured IPS SSM and the same setup should be followed except using the name SSM-40-B and the IP address of 10.4.240.28/27.

Summary

Agencies are exposed to a large number of threats from the Internet. Cisco IPS deployed in the Internet Edge of an agency plays a significant role in identifying and blocking malicious traffic and improves the availability and security of the Internet facing services.

Remote Access VPN

Agency Overview

Many agencies need to offer network connectivity to their data resources for users regardless of their location. Employees, contractors, and partners may need to access the network when traveling or working from home or from other off-site locations. The remote-access connectivity should support a wide variety of endpoint devices and provide seamless access to networked data resources. The remote-access connectivity should support authentication and policy control that integrates with the authentication resources in use by the agency. This connectivity should utilize cryptographic security to prevent the exposure of sensitive data to unauthorized parties who accidentally or intentionally intercept the data.

Technology Overview

The remote-access for remote users can be provided through one of the following methods:

- Software VPN client
- Hardware VPN client
- Secure Socket Layer (SSL) VPN web portal

The Cisco Adaptive Security Appliance (ASA) family supports IPsec, web portal, and full tunnel SSL VPNs for client-based remote access and IPsec for hardware client or site-to-site VPN. This section describes the basic configuration of remote access IPsec, web portal, and SSL VPNs for basic remote access, plus the configuration of Cisco Easy VPN for hardware client (ASA 5505) access.

Software clients such as the Cisco VPN Client and Cisco AnyConnect Client are recommended for remote users that require full network connectivity. The IPsec VPN client requires the user to have client software already loaded and configured on their machine in order to connect, and works best with agency-owned machines such as laptops. The Cisco AnyConnect client uses SSL and is designed for automated download and installation. SSL access can be more flexible and is likely to be accessible from more locations than IPsec, as few agencies block HTTPS access out of their networks.

A hardware client is a physical device like a small appliance or router that can provide an “always on” connection back to the agency network. They are typically used in situations where the user connects regularly, for long periods of time, from a static location, such as a home office user.

The SSL VPN web portal provides an SSL-based front-end to specific applications. This functions similar to a web proxy and is ideal for HTTP-based applications and simple file upload and download operations. With SSL, a restricted level of service can be offered when the user connects from unknown machines, thus providing greater security for the agency network.

The SBA for Large Agencies—Borderless Networks offers two different remote-access VPN designs:

- Remote-Access VPN (RAVPN) concentration integrated with firewall Cisco ASA pair for Internet Edge 5K design. This offers lower capital investment and reduces the numbers of devices the network engineering staff must manage.
- Remote-Access VPN concentration deployed on a pair of standalone Cisco ASA for the Internet Edge 10K design. This design offers greater operational flexibility and scalability, while providing a simple migration path from an existing RAVPN installation.

This document describes the configuration for remote access VPN via the SSL VPN WebVPN portal, as well as AnyConnect and IPsec clients. The configuration is broken into sections for each of the various access methods, and begins with a configuration that is common to all of the access methods. Configurations for both the Internet Edge 5K and Internet Edge 10K offer identical functionality and capability, so that regardless of design chosen, the user experience will be unchanged from one design to the other. Unless specifically noted, the configuration described in this document is common to both the Internet Edge 5K and Internet Edge 10K design.

Hardware applied in this design is selected based on the following performance values:

Cisco ASA Family Product	Maximum IPsec VPN Sessions	Maximum SSL VPN Sessions
Cisco ASA 5510	250	250
Cisco ASA 5520	750	750
Cisco ASA 5540	5000	2500

Remote Access VPN Configuration Details

The baseline configuration of the ASA including availability, routing, Internet, and inside connectivity, as well as management/administration access has already been covered in the “Firewall” section of this deployment guide.

If these aspects of this configuration are unfamiliar, review the relevant ‘Firewall’ sections.

The Cisco ASA's Remote Access VPN termination capabilities can be configured from the command line or from the graphical user interface Cisco Adaptive Security Device Manager (ASDM). Cisco ASDM provides a guided step-by-step approach to the configuration of RAVPN and reduces the likelihood of configuration errors.

This guide's complete Remote Access VPN configuration may be pasted into the CLI, then edit network-specific portions of the configuration with ASDM.

Remote Access VPN Configuration

Process

1. Global configuration
2. NAT Policy modification for Internet Edge 5K
3. Configure client pool route summarization
4. IPsec client configuration
5. WebVPN basic configuration and AnyConnect configuration
6. Hardware Client configuration

Procedure 1

Global Remote Access Configuration

This procedure sets up user authentication and global remote-access parameters that are common to all access methods.

Procedure Steps:

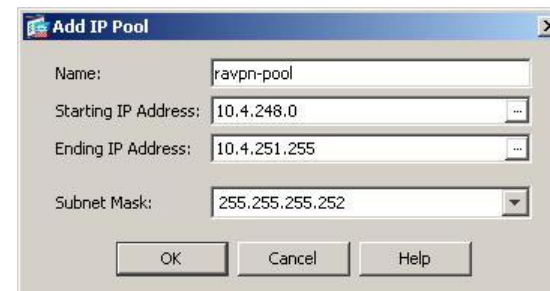
1. Configure address pools
2. Configure route summarization
3. Define default group policy
4. Configure Active Directory administrative account
5. Add VPN groups to Active Directory
6. Add users to VPN groups in Active Directory
7. Define AAA authentication parameters
8. Configure NAT exemption (for Internet Edge 5K design only)

Step 1: Configure address pools (Figure 62).

Open the **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools** panel. Define the Remote-Access VPN address pool that will be assigned to users when they connect to the VPN service:

This address-pool defines a sufficiently large address range to allow for 1022 users. If more address-space is needed, allocate a larger subnet, or define additional pools:

Figure 62. Add RAVPN IP Address Pool

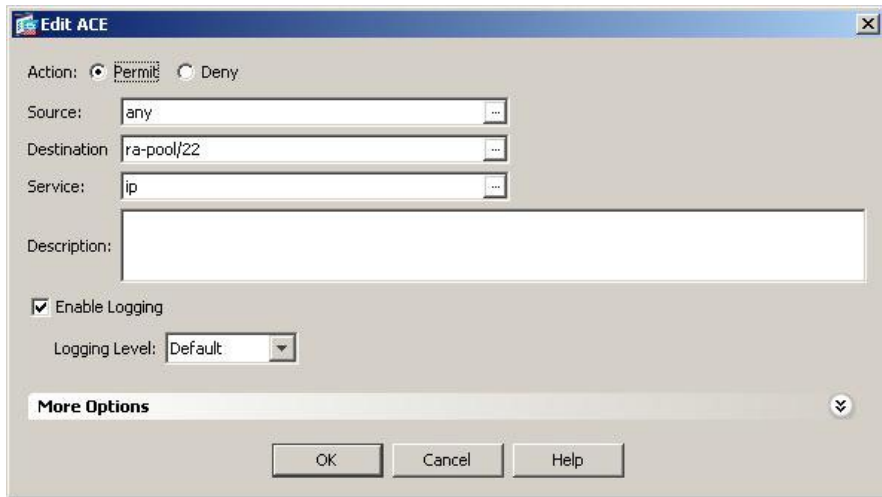


The screenshot shows a window titled "Add IP Pool" with a close button (X) in the top right corner. Inside the window, there are four input fields: "Name:" with the text "ravpn-pool", "Starting IP Address:" with the text "10.4.248.0", "Ending IP Address:" with the text "10.4.251.255", and "Subnet Mask:" with the text "255.255.255.252". At the bottom of the window, there are three buttons: "OK", "Cancel", and "Help".

Assign an object-group for the VPN pool in the **Configuration > Remote Access VPN > Network (Client) Access > Advanced > ACL Manager** panel (Figure 63).

Referring to the remote-access address-pool is more intuitive if it is assigned a relevant network name for the beginning address of the VPN pool.

Figure 63. Configure VPN Pool Access-List



Step 2: Configure route summarization on the adjacent switch for the remote-access VPN address-pool.

The Cisco ASA advertizes the remote-access address-pool to the rest of the network as individual hosts routes for each connected user. Summarizing the address-pool avoids the nuisance of the VPN clients' individual host routes propagating throughout the network.

```
interface TenGigabitEthernet1/0/1
ip summary-address eigrp 100 10.4.240.0 255.255.240.0 90
!
interface TenGigabitEthernet2/0/1
ip summary-address eigrp 100 10.4.240.0 255.255.240.0 90
```

Step 3: Define the **Default Group Policy (DfltGrpPolicy)** configuration in the **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** panel:

This section of the config carries attributes that are common to all VPN groups, such as the address pool (Figure 64), DNS servers (Figure 65), tunnel policy (Figure 66), the domain for split-tunnel name resolution, and which VPN services will be globally allowed for the various VPN groups. The default policy configuration may be overridden by more-granular configuration in the various VPN groups' description.

Figure 64. Default Group Policy: Address Pool



Figure 65. Default Group Policy: DNS Server

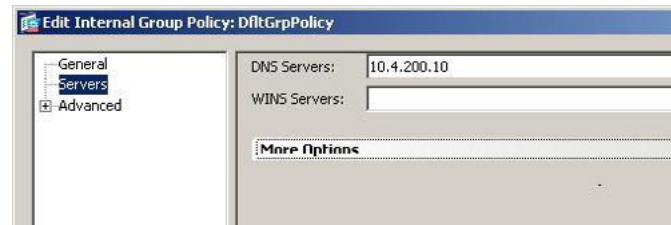
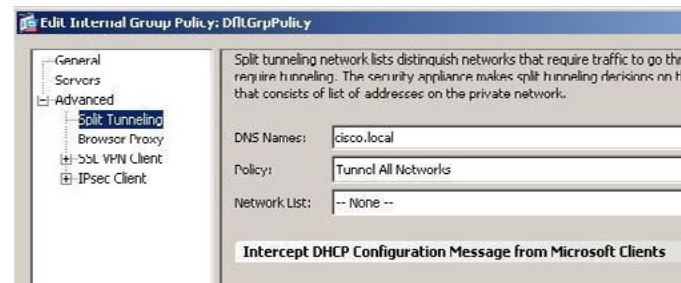


Figure 66. Default Group Policy: Split Tunneling Policy



Step 4: Use the Microsoft Windows server administrative tools to define Active Directory configuration in Steps 4 through 6. Configure the administrative account in Active Directory (Figure 67).

The administrative account provides the remote access concentrator's access to the Active Directory. This configuration is applied on the Windows Active Directory server.

Figure 67. Active Directory: Administrative Account

ASA 5520 Properties

Member Of | Dial-in | Environment | Sessions

Remote control | Terminal Services Profile | COM+

General | Address | Account | Profile | Telephones | Organization

First name: ASA Initials:

Last name: 5520

Display name: ASA 5520

Description:

Office:

Telephone number: Other...

E-mail:

Web page: Other...

OK Cancel Apply

Step 5: Add the relevant VPN groups to the Active Directory that will correspond to the various VPN access policies (Figure 68).

The Active Directory provides the users' group membership to the ASA as a return-attribute, along with a notification of success or failure for the users' credentials. This configuration is applied on the Windows Active Directory server.

Figure 68. Active Directory: Create Group for VPN Users

vpn-user Properties

General | Members | Member Of | Managed By

Group name (pre-Windows 2000): vpn-user

Description:

E-mail:

Group scope

☐ Domain local

☒ Global

☐ Universal

Group type

☐ Security

☒ Distribution

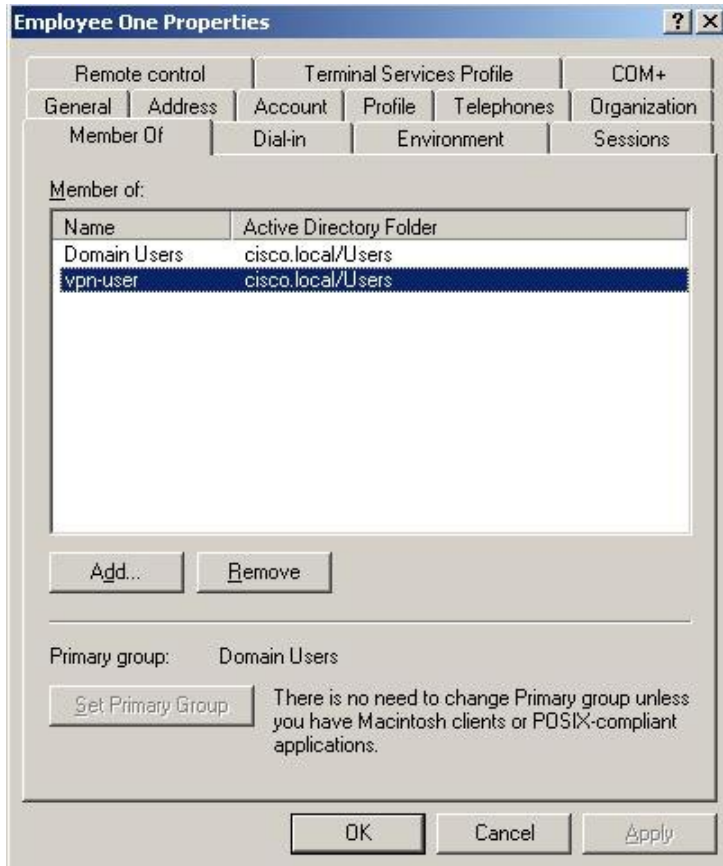
Notes:

OK Cancel Apply

Step 6: Add users to the appropriate VPN access group if they are to be allowed to access the Remote Access VPN (Figure 69).

This configuration is applied on the Windows Active Directory server.

Figure 69. Active Directory: Add Users to VPN Group

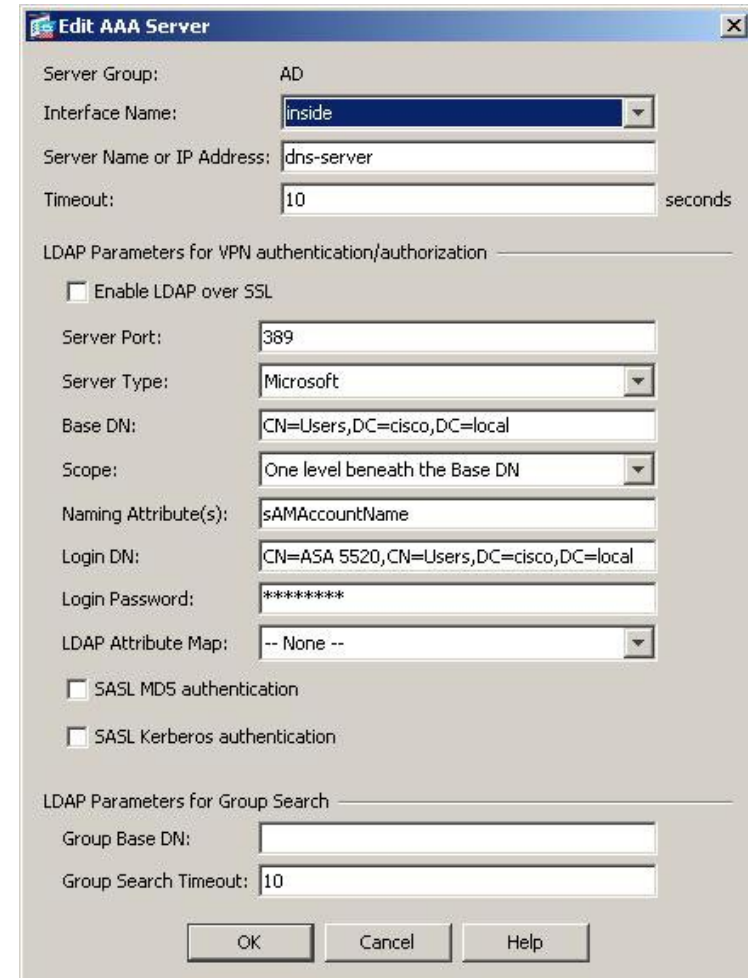


Step 7: Define the authentication group in the **Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups** panel (Figure 70).

Authentication is the portion of the configuration that verifies that users' credentials (username and password) match those stored within the agency's database of users that are allowed to access electronic resources. The SBA for Large Agencies—Borderless Networks uses Microsoft Active Directory for

its authentication database. When the Cisco ASA queries the Active Directory database to determine whether a user's name and password is valid to establish a Remote Access VPN connection, the Active Directory returns a VPN group-name attribute that the Cisco ASA applies to assign the user to the appropriate VPN access group. This requires configuration on the Active Directory Server to create a user with access to the directory, and additional configuration on the ASA to associate the values returned by Active Directory with locally significant group names.

Figure 70. LDAP Parameters for Active Directory Integration

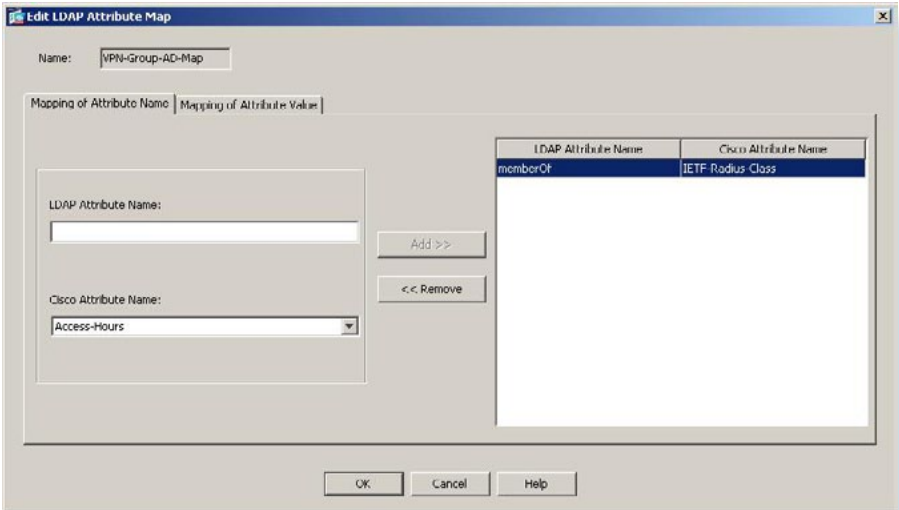


Step 8: Configure an LDAP attribute-map that associates vpn-group values returned from AD with local VPN Groups.

The LDAP attribute-map converts the LDAP return attributes to locally significant values. LDAP attribute-map configuration is found on the **Configuration > Remote Access VPN > AAA/Local Users > LDAP Attribute Map** panel.

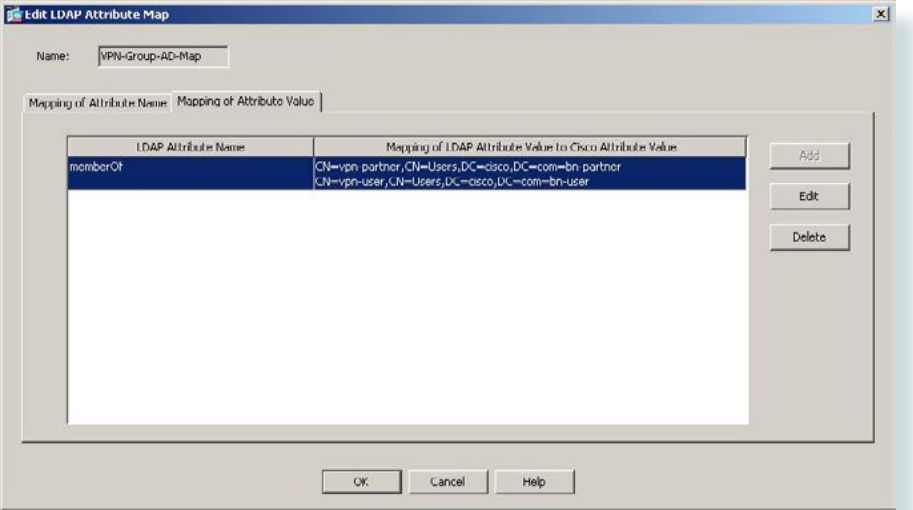
The 'Mapping of Attribute Name' panel defines which attributes will be mapped together (Figure 71).

Figure 71. Configure LDAP Attribute Map - Attribute Name



The 'Mapping of Attribute Value' panel defines which values (Directory VPN User Group names) to expect from the Active Directory server, and which local value (Cisco ASA VPN Group name) will be derived from the AD return-attribute (Figure 72).

Figure 72. Configure LDAP Attribute Map: Attribute Value

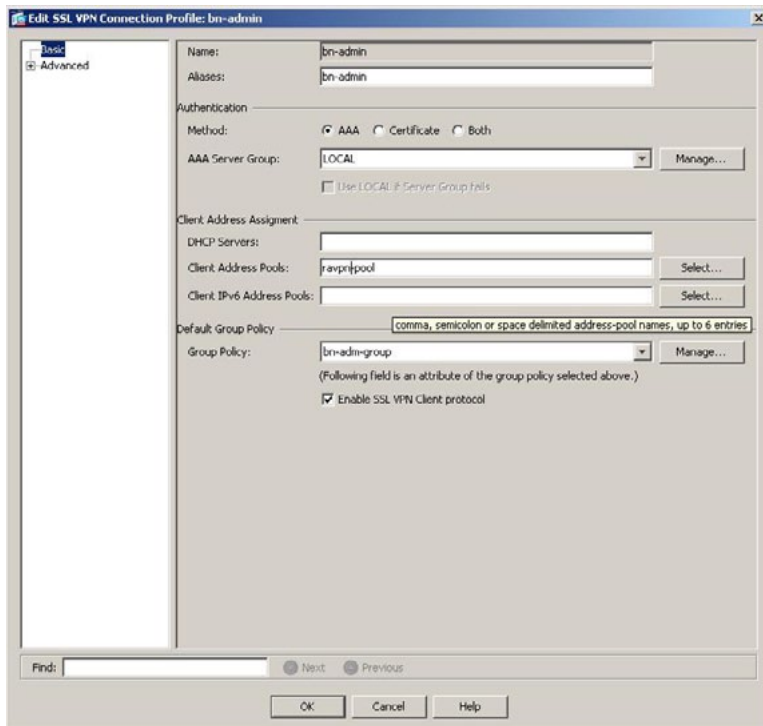


Step 9: Define tunnel policies and configure group-policies by browsing to **Remote Access VPN > Network (Client Access) > IPsec Connection Profiles**. Find the appropriate group name under 'Connection Profiles', and click 'Edit' (Figure 73).

A different VPN group is required for each remote-access policy. This design includes three VPN groups. All three groups use a full-tunnel policy in order to ensure that hosts that are infected with malware cannot be remote-controlled while connected to the VPN. The three groups differ in these respects:

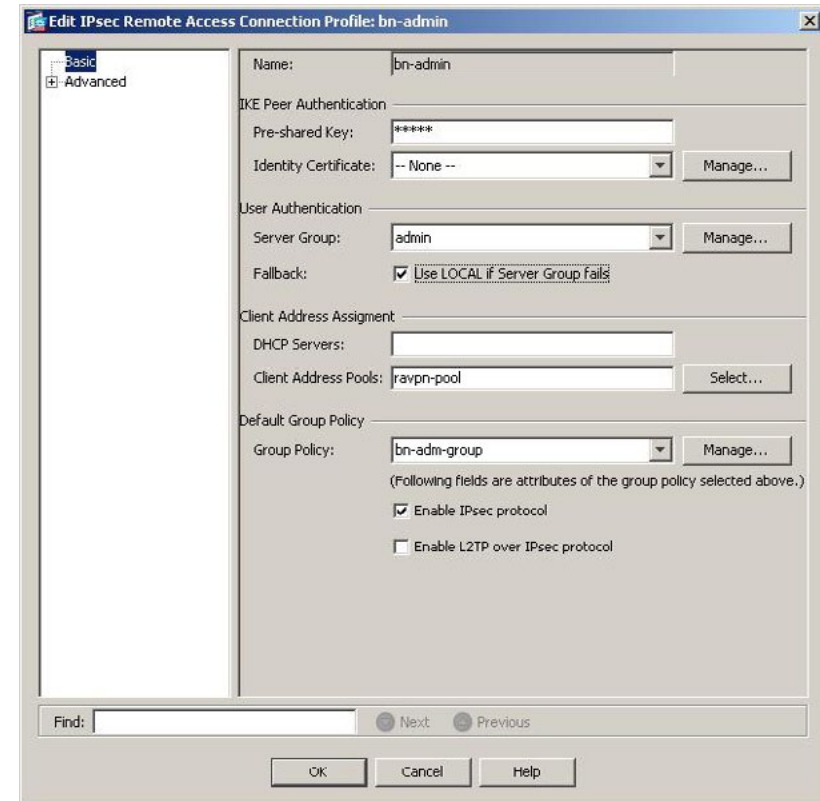
- Administrative users are authenticated by Active directory, or a local username and password can be checked. This ensures that VPN access is available when the Active Directory server is unavailable. Administrative users have full access to the entire network.
- Employees are authenticated by Active directory and have open access to the entire network
- Partners are authenticated by Active Directory and, although they use a tunnel-all VPN policy, there is an access-list applied to the tunnels to restrict access to specific hosts.

Figure 73. Configure Tunnel Policy



Step 10: Define the tunnel-group, which ties together the LDAP group return attribute, the group tunnel policy, and the address-pool that will be used by the tunnel-group.

Figure 74. Associate group policy with AAA values



Executing the preceding steps in ASDM will apply this Cisco ASA Command-Line Interface configuration:

```
ip local pool [ravpn-pool] [ra-pool]-[10.4.251.255] mask
[255.255.252.0]
names
name [10.4.248.0] [ra-pool]
group-policy [DfltGrpPolicy] attributes
  dns-server value [10.4.200.10]
  vpn-tunnel-protocol IPSec svc webvpn
  split-dns value [cisco.local]
  address-pools value [ravpn-pool]
aaa-server [AD] protocol [ldap]
```



```

aaa-server [AD] ([inside]) host [dns-server]
server-port [389]
ldap-base-dn CN=[Users],DC=[Cisco],DC=[local]
ldap-naming-attribute sAMAccountName
ldap-login-password [cisco]
ldap-login-dn CN=[ASA 5520],CN=[Users],DC=[Cisco],DC=[local]
server-type [Microsoft]ldap attribute-map [VPN-Group-AD-Map]
map-name memberOf IETF-Radius-Class
map-value memberOf CN=[vpn-partner],CN=[Users],DC=[cisco],DC
=[com] [bn-partner]
map-value memberOf CN=[vpn-user],CN=[Users],DC=[cisco],DC=[c
om] [bn-user]group-policy [bn-adm-group] internal
group-policy [bn-adm-group] attributes
split-tunnel-policy tunnelspecified
split-tunnel-network-list value [RA_FullTunnelACL]
group-policy [bn-user-group] internal
group-policy [bn-user-group] attributes
split-tunnel-policy tunnelspecified
split-tunnel-network-list value [RA_FullTunnelACL]
group-policy [bn-partner-group] internal
group-policy [bn-partner-group] attributes
split-tunnel-policy tunnelspecified
split-tunnel-network-list value [RA_FullTunnelACL]
tunnel-group [bn-user] type remote-access
tunnel-group [bn-user] general-attributes
address-pool [ravpn-pool]
authentication-server-group [AD]
default-group-policy [bn-user-group]
tunnel-group [bn-admin] type remote-access
tunnel-group [bn-admin] general-attributes
address-pool [ravpn-pool]
default-group-policy [bn-adm-group]
tunnel-group [bn-partner] type remote-access
tunnel-group [bn-partner] general-attributes
address-pool [ravpn-pool]
authentication-server-group [AD]
default-group-policy [bn-partner-group]
access-list [inside_nat0_outbound]
extended permit ip [10.4.0.0] [255.254.0.0] [10.4.252.0]
[255.255.252.0]

```

Procedure 2

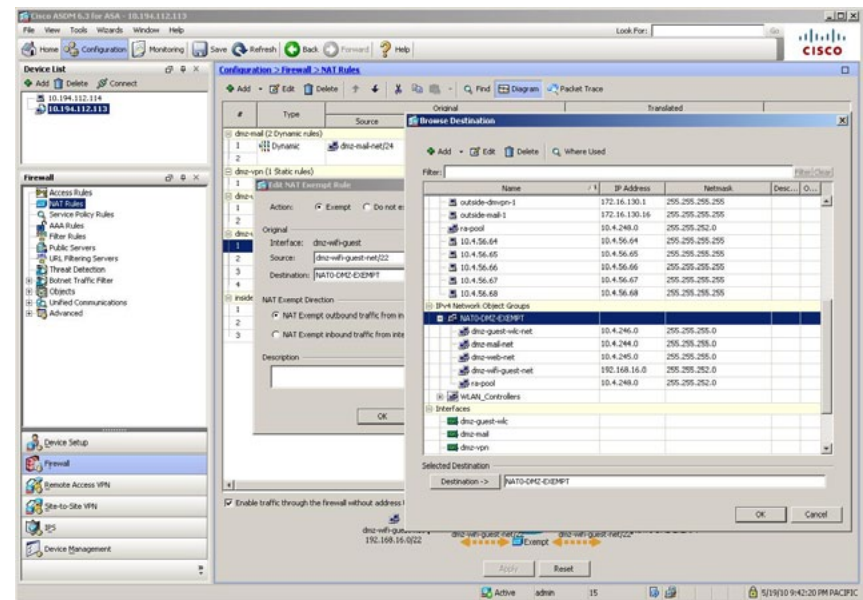
Configure NAT Exemption

The Internet Edge 5K Design cannot NAT the traffic to the Remote-Access VPN users, or their traffic will not work. This step is not required by the Internet Edge-10K design.

Step 1: Configure NAT Exemption for RAVPN User Pool by browsing to Firewall > NAT Rules (Figure 75).

In the Internet Edge 5K design, NAT exemption must be configured for traffic from the LAN that is going to the remote access clients. If this were not configured, traffic to clients would end up being translated, which would change the source address of the traffic, making it impossible for clients to receive traffic correctly from servers that they communicate with. This step is not needed on the Internet Edge 10K design because the VPN function is separated from the Internet Firewall functionality in that design, and NAT is not implemented on the VPN-only ASA.

Figure 75. Add NAT Exemption for RA VPN address pool



Procedure 3 Configure Route Summarization

This procedure adds routing configuration to the adjacent distribution switch to minimize the number of routes that must be advertised to the rest of the network for the VPN client pool.

Procedure Steps:

1. Configure route summarization

Step 1: Configure route summarization on the adjacent switch for the remote-access VPN address-pool.

The Cisco ASA advertizes the remote-access address-pool to the rest of the network as individual hosts routes for each connected user. Summarizing the address-pool avoids the nuisance of the VPN clients' individual host routes propagating throughout the network.

```
interface TenGigabitEthernet1/0/1
ip summary-address eigrp 100 10.4.240.0 255.255.240.0 90
!
interface TenGigabitEthernet2/0/1
ip summary-address eigrp 100 10.4.240.0 255.255.240.0 90
```

Procedure 4 IPsec Configuration

The following configuration enables user access to the network via the Cisco IPsec VPN Client. This configuration requires the configuration described above in the “Global Remote Access Configuration.”

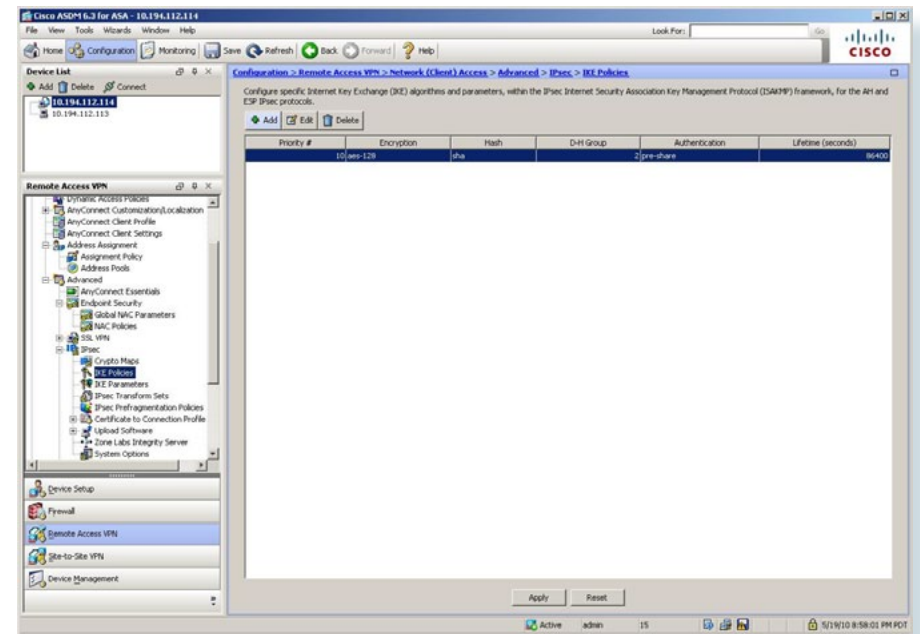
Procedure Steps:

1. Configure Head-End ISAKMP and IPSec Policies
2. Configure Remote Access Connection Profile
3. Configure IPSec VPN Client

Step 1: Configure the Remote Access ISAKMP and IPsec Policies (Figure 76).

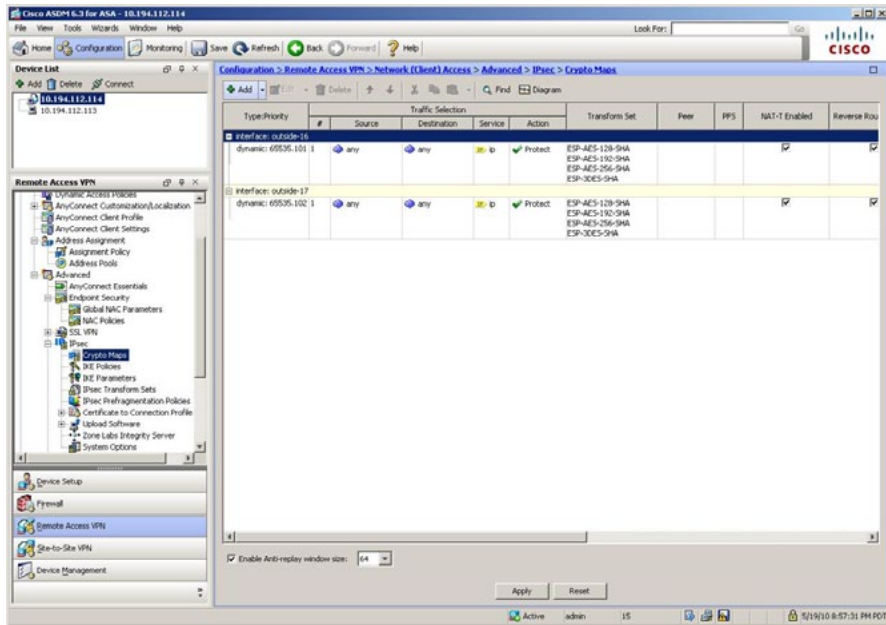
ISAKMP policies define the protection that is applied for the initial connection from IPsec VPN Clients to the Cisco ASA.

Figure 76. Create ISAKMP Policy



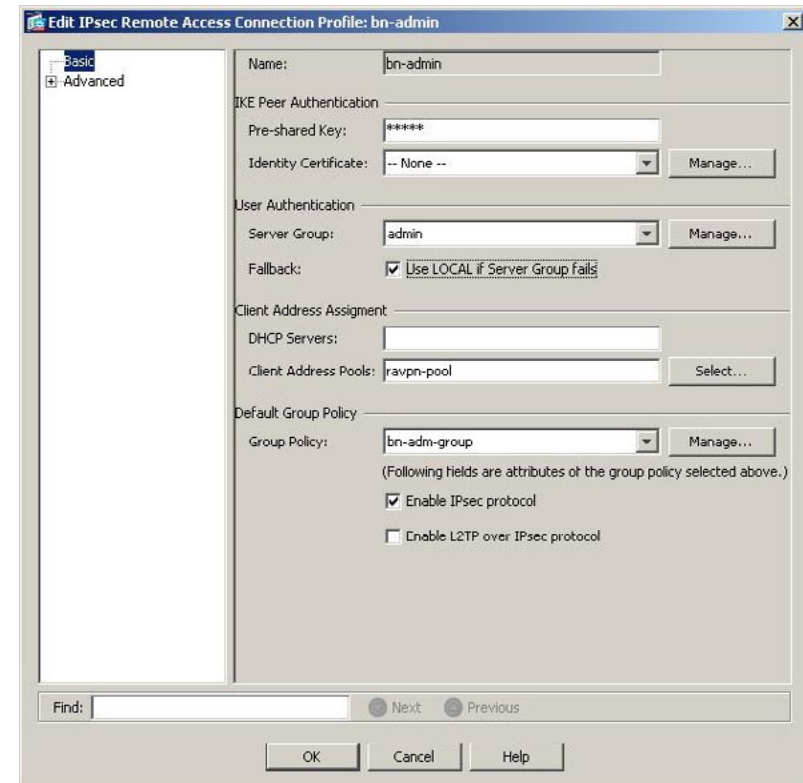
IPsec policies define the cryptographic protection that is applied for remote access VPN users' data connectivity.

Figure 77. Create IPsec Policies



Step 2: Add IPsec VPN Client Remote Access connection profile (Figure 78). The remote VPN client inherits a significant portion of its configuration from the RAVPN headend.

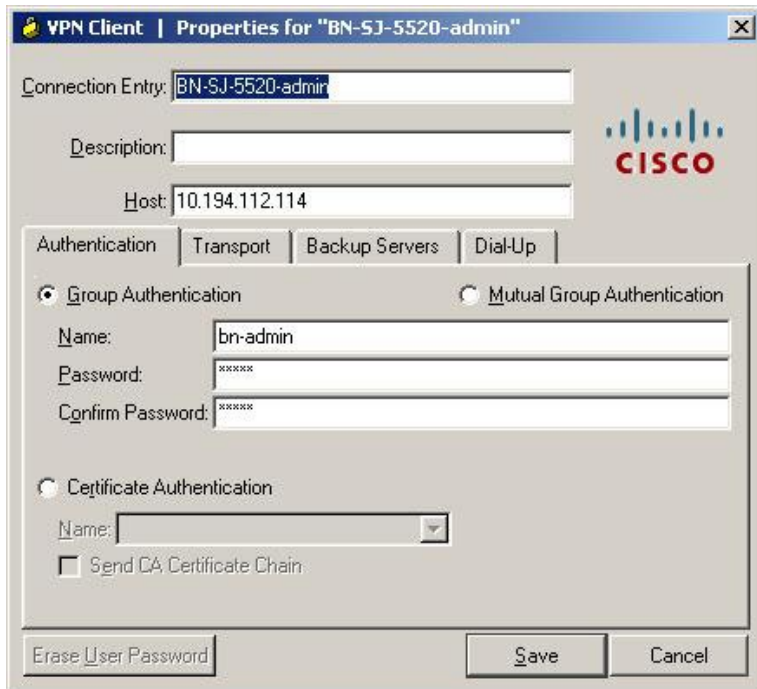
Figure 78. Head-End Remote Access Connection Profile



Step 3: Configure the IPsec VPN Client to connect to the appropriate VPN group (Figure 79).

The IPsec VPN client need to be configured to match the parameters on the VPN headend. On the client side for IPsec, the user needs the IP address or DNS name of the headend, the group name and password, and a username and password.

Figure 79. IPsec VPN Client Configuration



Executing the preceding steps in ASDM will apply the following CLI configuration:

```
crypto isakmp enable [outside-16]
crypto isakmp enable [outside-17]
crypto isakmp policy 10
  authentication pre-share
  encryption aes
  hash sha
  group 2
  lifetime 86400
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
crypto dynamic-map [BN_DYN_CRYPTO_MAP_1] 101 set transform-set ESP-AES-128-SHA ESP-AES-192-SHA ESP-AES-256-SHA ESP-3DES-SHA
crypto dynamic-map [BN_DYN_CRYPTO_MAP_1] 101 set reverse-route
crypto dynamic-map [BN_DYN_CRYPTO_MAP_2] 102 set transform-set ESP-AES-128-SHA ESP-AES-192-SHA ESP-AES-256-SHA ESP-3DES-SHA
crypto dynamic-map [BN_DYN_CRYPTO_MAP_2] 102 set reverse-route
crypto map [outside-16_map] 65535 ipsec-isakmp dynamic [BN_DYN_CRYPTO_MAP_1]
crypto map [outside-16_map] interface [outside-16]
crypto map [outside-17_map] 65535 ipsec-isakmp dynamic [BN_DYN_CRYPTO_MAP_2]
crypto map [outside-17_map] interface [outside-17]
tunnel-group [bn-user] ipsec-attributes
  pre-shared-key [c1sco123]
tunnel-group [bn-admin] ipsec-attributes
  pre-shared-key [c1sco123]
tunnel-group [bn-partner] ipsec-attributes
  pre-shared-key [c1sco123]
```

Procedure 5 AnyConnect Configuration

Procedure Steps:

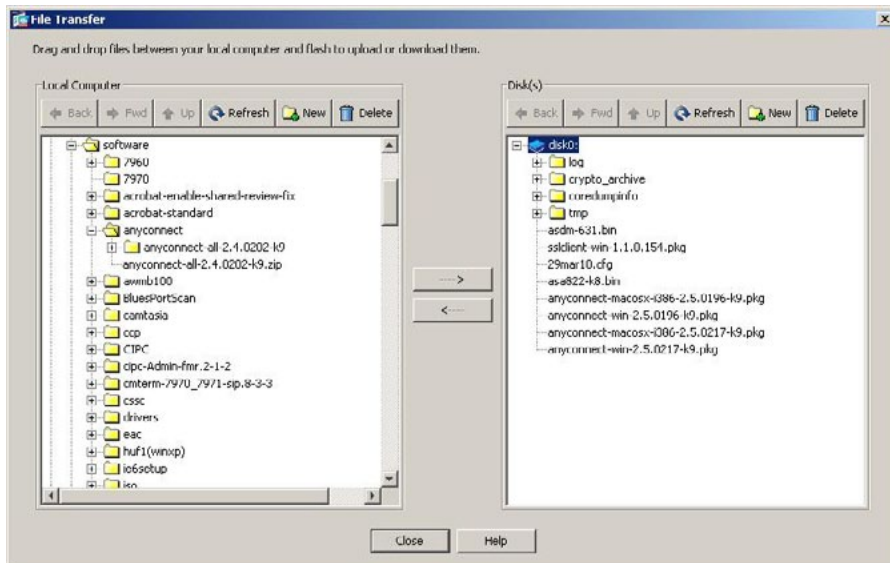
1. Upload AnyConnect Client Binaries to Head-End ASA
2. Global WebVPN Configuration
3. Create WebVPN Group Connection URLs
4. AnyConnect Client Configuration

The Cisco ASA requires specific configuration to enable AnyConnect client support.

Step 1: Upload the appropriate platforms' anyconnect clients to the ASAs using the File Transfer tool, found in the **Tools > File Management** menu. Select the **Between Local PC and Flash...** in the **File Transfer** button (Figure 80).

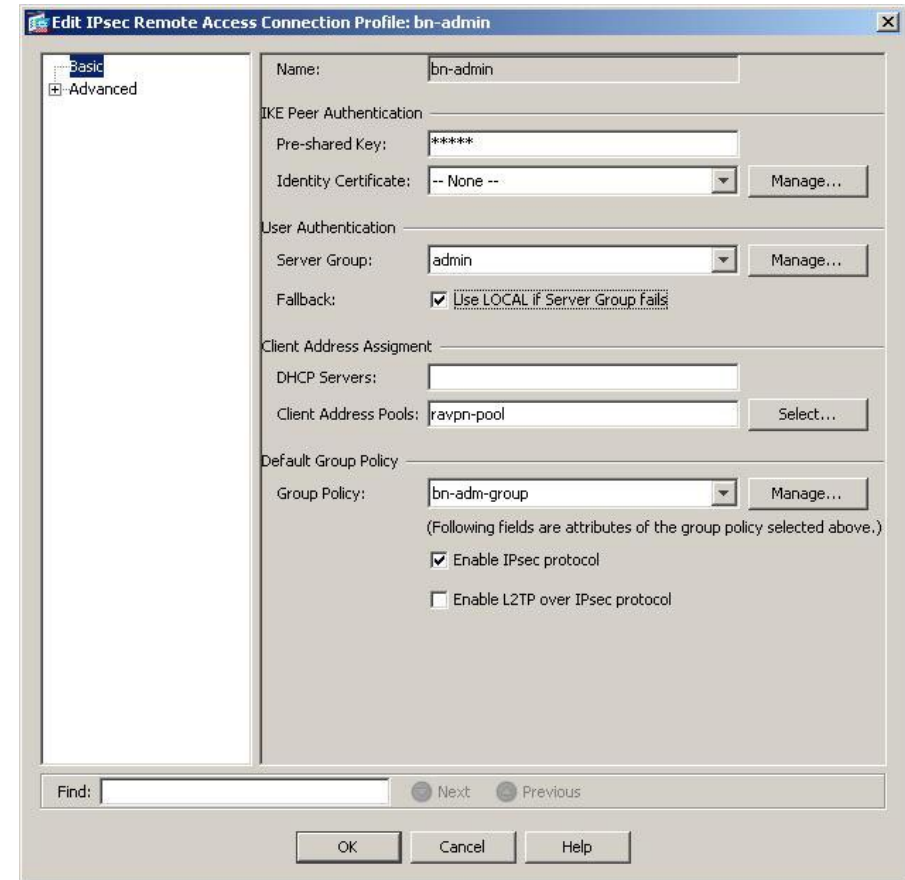
The AnyConnect client binaries are available for download on Cisco.com; download all clients needed to support the hardware and software platforms that are in use within the agency. Upload the files to both ASAs in the High Availability pair.

Figure 80. Upload AnyConnect Binary to ASA



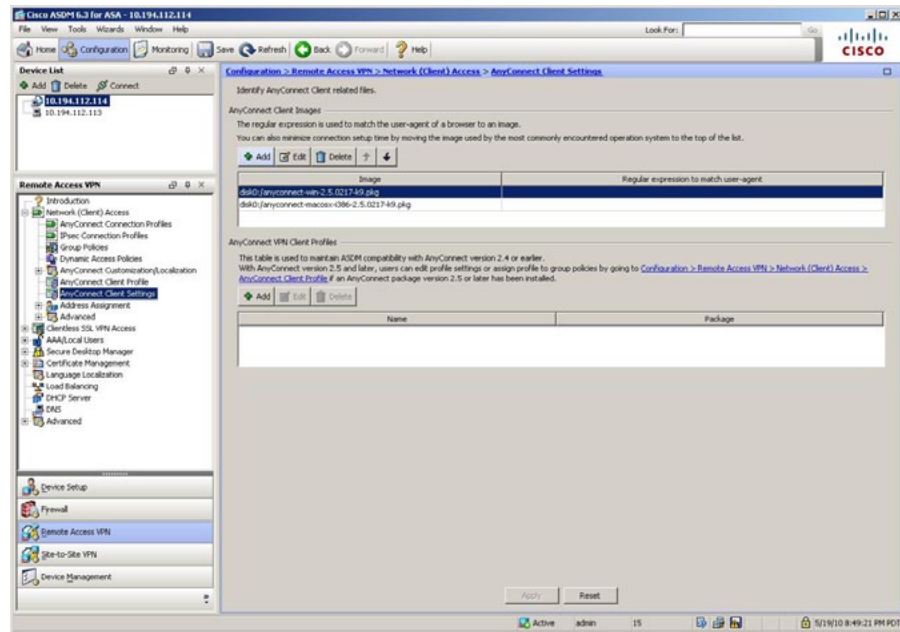
Step 2: Add global WebVPN configuration to the Default Group Policy (DfltGrpPolicy) configuration (Figure 81).

Figure 81. Configure AnyConnect Client Policy



Step 3: Once uploaded, assign the current version of the active AnyConnect client (Figure 82).

Figure 82. Define AnyConnect Client

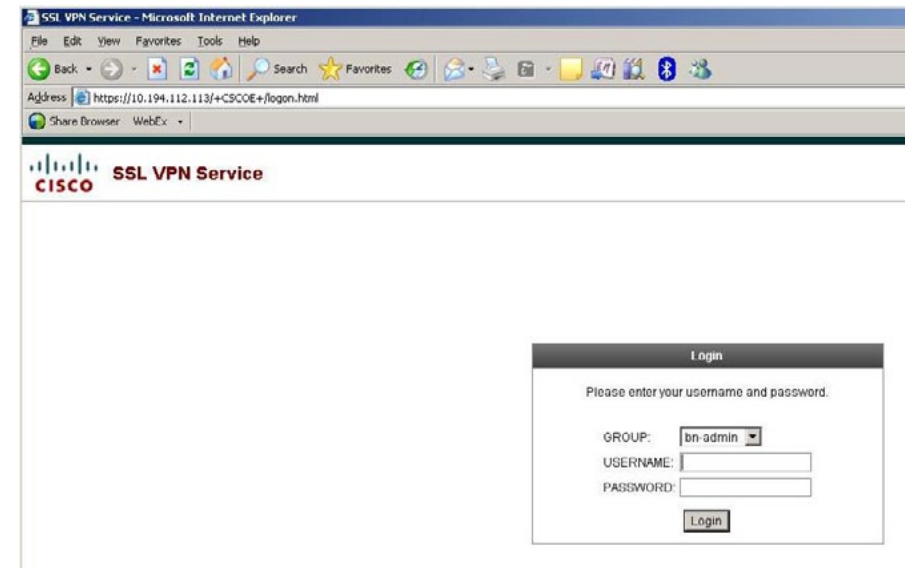


Step 4: Create WebVPN Group Connection URLs

By defining specific connection URL aliases, users can connect directly to their respective VPN group instead of needing to select their group on the login screen. If using the Internet Edge 10K design with dual ISP connections, expect to offer VPN connectivity through both ISP connections, be sure to provide group-urls for the IP address or hostnames for both ISPs. Open a web browser on the client PC and connect to the group-url.

The AnyConnect client's initial connection is typically launched with a web browser. After the client is installed on a user's computer, subsequent connections can be established through the web browser again, or directly through the AnyConnect client, which is now installed on the user's computer. The user needs the IP address or DNS name of the Cisco ASA, a username and password, and the name of their VPN group that they are assigned to. Alternatively, the user can directly access their VPN group with their group-url, after which they will need to provide their username and password.

Figure 83. AnyConnect Client Initiation via WebVPN Portal



Executing the preceding steps in ASDM will apply this Cisco ASA Command-Line Interface configuration:

```
group-policy [DfltGrpPolicy] attributes
webvpn
  svc ask none default svc
webvpn
  enable [outside-16]
  enable [outside-17]
  anyconnect-essentials
  svc image [disk0]:/[anyconnect-win-2.5.0196-k9.pkg] [1]
  svc image [disk0]:/[anyconnect-macosx-i386-2.5.0196-k9.pkg]
[2]
  svc enable
  tunnel-group-list enable
tunnel-group [bn-user] webvpn-attributes
  group-alias [bn-user] enable
  group-url https://[10.194.112.114]/[bn-user] enable
  group-url https://[10.194.112.118]/[bn-user] enable
tunnel-group [bn-admin] webvpn-attributes
  group-alias [bn-admin] enable
  group-url https://[10.194.112.114]/bn-admin enable
  group-url https://[10.194.112.118]/bn-admin enable
tunnel-group [bn-partner] webvpn-attributes
  group-alias [bn-partner] enable
  group-url https://[10.194.112.114]/[bn-partner] enable
  group-url https://[10.194.112.118]/[bn-partner] enable
```

Procedure 6

Hardware Client Configuration

Telecommuters or other users that will use multiple devices including IP phones or other platforms that cannot use a VPN client to offer remote-site connectivity can use a 'hardware client' device to connect their remote location to agency IT resources with cryptographic security. The hardware-client configuration applies a slightly different VPN connection mode, called 'Network Extension Mode,' wherein devices on the remote network are configured within the IP address range of the agency's network (within the remote-access VPN pool, in this case).

Procedure Steps:

1. Configure Network Extension Mode Policy
2. Configure Local Authentication
3. Configure a Cisco ASA 5505 Hardware Client

Step 1: Enable Network Extension Mode.

```
group-policy 5505Group internal
group-policy 5505Group attributes
  vpn-tunnel-protocol IPSec
  ip-comp enable
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value [RA_SplitTunnelACL]
  user-authentication-idle-timeout 480
  nem enable
username 5505site5 password cisco123
username 5505site5 attributes
  vpn-group-policy 5505Group
tunnel-group RA5505 type remote-access
tunnel-group RA5505 general-attributes
  default-group-policy 5505Group
tunnel-group RA5505 ipsec-attributes
  pre-shared-key cisco123
```


Step 2: Define local authentication for the telecommuter connections.

Local authentication offers an effective solution for telecommuter VPN connections, because the telecommuter credentials are only relevant to remote-access connections that terminate on the single pair of ASAs, unlike other remote-access connections that apply network usernames that have relevance for many other network services.

```
username 5505site5 password c1sco123
username 5505site5 attributes
vpn-group-policy 5505Group
```

Step 3: Configure a Cisco ASA 5505 Hardware Client

The ASA will support a wide variety of routers as VPN hardware remote clients as well as the ASA 5505. In this example, we are using the ASA 5505 for the remote hardware client. Apply the following text to completely configure connectivity for an ASA 5505:

```
hostname 5505Site32
domain-name cisco.local
enable password c1sco123
passwd c1sco123
names
!
interface Vlan1
 nameif inside
 security-level 100
 ip address [10.4.251.249] [255.255.255.248]
!
interface Vlan2
 nameif outside
 security-level 0
 ip address dhcp setroute
!
interface Ethernet0/0
 no shut
!
interface Ethernet0/1
 no shut
!
interface Ethernet0/2
 no shut
!
interface Ethernet0/3
 no shut
!
interface Ethernet0/4
```

```
no shut
!
interface Ethernet0/5
 no shut
!
interface Ethernet0/6
 no shut
!
interface Ethernet0/7
 switchport access vlan 2
 no shut
!
dns server-group DefaultDNS
 domain-name [cisco.local]
http server enable
http [10.4.0.0] [255.254.0.0] [inside]
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
crypto isakmp policy 65535
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
telnet 10.4.0.0 255.254.0.0 inside
telnet timeout 5
ssh 10.4.0.0 255.254.0.0 inside
ssh timeout 5
ssh version 2
console timeout 0
management-access inside
dhcpd auto_config outside
dhcpd option 150 ip 10.4.200.20
!
dhcpd address 10.4.251.250-10.4.251.254 inside
dhcpd dns 10.4.200.10 interface inside
dhcpd domain cisco.local interface inside
dhcpd enable inside
!
vpnclient server 10.194.112.114
vpnclient mode network-extension-mode
vpnclient nem-st-autoconnect
vpnclient vpngroup RA5505 password c1sco123
vpnclient username 5505site5 password c1sco123
vpnclient enable
!
username admin password c1sco123 privilege 15
```

Remote Access VPN Summary

The Cisco ASA supports IPsec, web portal, and full tunnel SSL VPNs for client-based remote access and IPsec for hardware client or site-to-site VPN. This section described the basic configuration of remote access IPsec, web portal, and SSL VPNs for basic remote access, plus the configuration of Cisco EZVPN for hardware client (ASA 5505) access.

Notes

Email Security

Agency Overview

Email is a critical service in most agencies. Failing to protect that service can result in a loss of data and employee productivity.

There are two major problems with email in networks today. The first issue is that floods of unsolicited email, commonly referred to as spam, waste employee time (because of the sheer volume of messages), and waste network bandwidth and storage.

Another problem is that large numbers of emails are malicious and contain malware or phishing attacks that try to deceive users into releasing sensitive information such as credit card numbers, social security numbers, or intellectual property.

Technology Overview

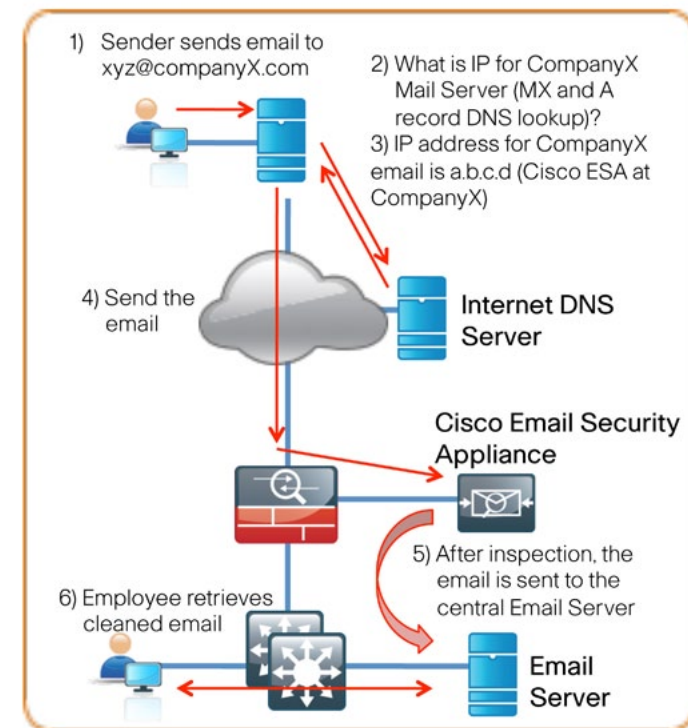
An email solution will become unusable if junk email is not filtered properly. The sheer volume of spam messages crowd out legitimate mail and cause employees to waste time manually filtering through messages. A side effect of some junk email-filtering solutions are false positives, or email that is incorrectly identified as spam causing legitimate messages to be discarded.

When this occurs the agency must sift through the junk email looking for legitimate messages or lower the level of filtering allowing more potential junk messages to go to users, making the user responsible for determining whether emails are spam. Unsolicited email is also more likely to be malicious and include embedded attacks. Criminal agencies are using attacks in email as an effective and cheap way to attack user machines. An example of an attack contained within email is malware that attempt to infect the host machine or that offer users counterfeit URLs (phishing) to trick them into going to a website where criminals can steal bank login credentials or infect the host machine.

The objective of these types of attacks are to gather social security numbers, credit card numbers, or to compromise the host to use it as a launch point to send spam and other attacks.

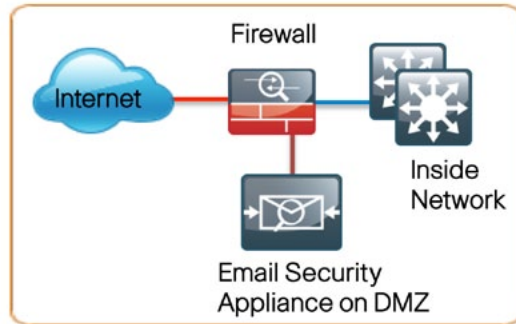
The Cisco IronPort® C-Series Email Security Appliance (ESA) protects the email infrastructure and employees who use email at work by filtering unsolicited and malicious email before it reaches the user. ESA easily integrates into existing email infrastructures with a high degree of flexibility. It does this by acting as a Mail Transfer Agent (MTA) within the email delivery chain. Another name for an MTA is a mail relay. A normal email exchange when an agency is using an MTA (mail relay) might look like the message flow shown below (Figure 84).

Figure 84. Email Message Flow



ESA can be deployed with a single physical interface to filter email to and from an agency's mail server. The second deployment option is a two-interface configuration, one interface for email transfers to and from the Internet and the other for email transfers to and from the internal servers. The Internet Edge design uses the single interface model for simplicity (Figure 85).

Figure 85. Cisco E-mail Security Appliance Deployment Overview



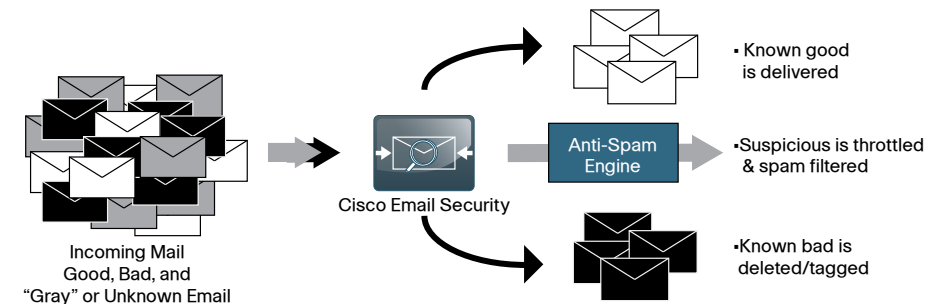
ESA uses a variety of mechanisms for spam and antivirus filtering. There are two ways to filter spam: reputation-based and context-based. Reputation filters provide the first layer of defense by looking at the source IP address of the email server and comparing this to the reputation data downloaded from Cisco SenderBase®. SenderBase is the world's largest repository for security data, including spam sources, botnets, and other malicious hosts. When hosts on the Internet engage in malicious activity, SenderBase lowers the reputation of that host. Devices like ESA that use reputation get updates several times a day from SenderBase. When ESA receives an email, it compares the source IP to the database provided by SenderBase. If the reputation of the sender is positive, the email gets forwarded on to the next layer of defense. If it is negative, the email is discarded. If the reputation falls in between, the email is considered suspicious and is quarantined and waits for inspection before being delivered (Figure 86).

Context-based antispam inspection in ESA inspects the entire mail message, including attachments, looking for details like sender identity, message content, embedded URLs, and email formatting. Using these algorithms, the ESA can identify spam messages without blocking legitimate email.

Cisco IronPort Email Security Appliance uses a multilayer approach to fight viruses. The first layer is the Virus Outbreak Filters. Virus Outbreak Filters are downloaded from SenderBase by the appliance. They contain a list of known bad mail servers. These filters are generated by watching global email traffic patterns that look for anomalies associated with an outbreak. When an email is received from a server on this list, it is kept in quarantine until the antivirus signatures are updated to counter the current threat.

The second layer of defense that ESA uses is antivirus (AV) signatures to scan quarantined emails to ensure that they do not carry viruses into the network.

Figure 86. Email Filtering Overview



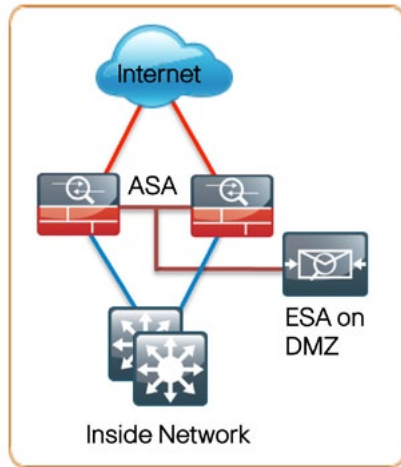
Configuration Details

Cisco ESA deployment is designed to be as easy as possible. It is deployed into the existing mail delivery chain as a Mail Transfer Agent (MTA). The ESA will be the destination of email for the agency; as such, the public MX records (the DNS record that defines where to send mail) must eventually point to the public IP address of the ESA.

In this deployment guide, the ESA is physically deployed on the DMZ of the Internet Edge firewall using a single interface for simplicity. This interface handles all incoming and outgoing email and carries management traffic. The port on the ESA is the M1 management interface (Figure 87).

It is important that the ESA be accessible through the public Internet and that it is the first hop in the email infrastructure. The sender IP address is used by several of ESA processes and is one of the primary identifiers SenderBase uses to determine the reputation of the sender. If another device receives mail before forwarding it to the ESA, the ESA will not be able to determine the sender IP address and filtering cannot be applied properly.

Figure 87. E-mail Security Appliance Deployment



Process

1. Initial ESA Deployment
2. System Updates and Feature Keys
3. Setup Bounce Verification
4. Set Mail Policies to drop SPAM

Procedure 1 Initial ESA Deployment

1. DNS Configuration
2. Initial Setup Options
3. Configure Management Access
4. Alternate (GUI Management Access Configuration)
5. System Setup Wizard
6. System Configuration
7. Network Integration
8. Message Security
9. Finalize Initial Configuration

Step 1: DNS Configuration

The ESA hostname is the name carried in the DNS Mail Exchange (MX) record and indicates that the ESA is the primary MTA. The DNS A (IP address) record is the public IP address for the ESA (in this case, the statically mapped public address on the firewall for the ESA that resides on the DMZ in Figure 5).

172.16.130.16 is the public address in ISP A to send email to cisco.local

This external address is statically NAT'ed back to dmz-mail interface to the ESA (which has an actual address of 10.4.244.16).

The MX records for cisco.local point to the 172.16.130.16 address as it is the public address (specific to this lab only) that other agencies use to send email.

After physically installing and connecting the ESA to the network, the next step is initial setup.



Tech Tip

The default username and password are admin/ironport.

Step 2: Initial Setup Options

The first step in deploying the ESA is to complete the System Setup Wizard by accessing the ESA Graphical User Interface (GUI) through a web browser.

If the agency's install procedures allow a PC to directly connect to the ESA via its default IP address, then skip ahead to the section titled "System Setup Wizard."

If the installation procedure requires the ESA to be rack mounted in a remote room, and the initial configuration to be performed remotely using an out-of-band connection such as serial port, then the ESA will need to be preconfigured with basic network settings. These settings are explained in the "Out-of-Band Network Configuration" section. Once complete, continue the setup by using the "System Setup Wizard."

Step 3: Configuring Management Access

To change the default network settings via a serial console port, connect using a standard null modem cable with the terminal emulator settings of 8-1-none-9600 baud. Once connected and logged in, run **interfaceconfig** and **setgateway** to change the basic network settings. Issue the **commit** command to save the changes to the running configuration.



Tech Tip

Depending on the code version the appliance has installed, the CLI or GUI interfaces might display slightly different options.

```
ironport.example.com> interfaceconfig
```

Currently configured interfaces:

```
1. Management (192.168.42.42/24 on Management: ironport.  
example.com)
```

Choose the operation you want to perform:

- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.

```
[> edit
```

Enter the number of the interface you wish to edit.

```
[> 1
```

IP interface name (Ex: "InternalNet"):

```
[Management]> Mail_DMZ
```

IP Address (Ex: 192.168.1.2):

```
[192.168.42.42]> 10.4.244.16
```

Ethernet interface:

1. Data 1
 2. Data 2
 3. Data 3
 4. Management
- ```
[4]>
```

Netmask (Ex: "255.255.255.0" or "0xffffffff"):

```
[255.255.255.0]> 255.255.255.0
```

Hostname:

```
[ironport.example.com]> c370.cisco.local
```

Do you want to enable FTP on this interface? [N]>

Do you want to enable Telnet on this interface? [Y]> **n**

Do you want to enable SSH on this interface? [Y]>

Which port do you want to use for SSH?

```
[22]>
```

Do you want to enable HTTP on this interface? [Y]>

Which port do you want to use for HTTP?

```
[80]>
```

Do you want to enable HTTPS on this interface? [Y]>

Which port do you want to use for HTTPS?

```
[443]>
```

Do you want to enable Spam Quarantine HTTP on this interface?

```
[N]> y
```

Which port do you want to use for Spam Quarantine HTTP?

```
[82]>
```

Do you want to enable Spam Quarantine HTTPS on this interface?

```
[N]> y
```

Which port do you want to use for Spam Quarantine HTTPS?

```
[83]>
```

You have not entered an HTTPS certificate. To assure privacy, run "certconfig" first. You may use the demo, but this will not be secure.



Do you really wish to use a demo certificate? [Y]>  
 Both HTTP and HTTPS are enabled for this interface, should  
 HTTP requests redirect to the secure service? [Y]>

Both Spam Quarantine HTTP and Spam Quarantine HTTPS are  
 enabled for this interface, should Spam Quarantine HTTP  
 requests redirect to the secure service? [Y]>

Do you want MAIL\_DMZ as the default interface for Spam  
 Quarantine? [N]> **y**

Do you want to use a custom base URL in your Spam Quarantine  
 email notifications? [N]>

The interface you edited might be the one you are currently  
 logged into. Are you sure you want to change it? [Y]>

Currently configured interfaces:  
 1. MAIL\_DMZ (10.4.244.16/24 on Management: c370.cisco.local)

Choose the operation you want to perform:

- NEW - Create a new interface.
  - EDIT - Modify an interface.
  - GROUPS - Define interface groups.
  - DELETE - Remove an interface.
- [ ]>

Please run "systemsetup" or "sethostname" then "commit" before  
 sending mail.  
 ironport.example.com> **setgateway**

Warning: setting an incorrect default gateway may cause the  
 current  
 connection to be interrupted when the changes are committed.  
 Enter new default gateway:  
 [ ]> 10.4.244.1

Please run "systemsetup" or "sethostname" then "commit" before  
 sending mail.  
 ironport.example.com> **commit**

Please enter some comments describing your changes:  
 [ ]> **initial setup**

Changes committed: Thu Apr 29 21:20:57 2010 UTC

After configuring the ESA, it should be able to ping the appliance from the  
 network, assuming the correct firewall rules have been applied.

ironport.example.com> ping 10.4.244.1

Press Ctrl-C to stop.

PING 10.4.244.1 (10.4.244.1): 56 data bytes  
 64 bytes from 10.4.244.1: icmp\_seq=0 ttl=255 time=0.481 ms  
 64 bytes from 10.4.244.1: icmp\_seq=1 ttl=255 time=0.271 ms  
 64 bytes from 10.4.244.1: icmp\_seq=2 ttl=255 time=0.195 ms

### Step 3: Alternate (GUI Management Access Configuration)

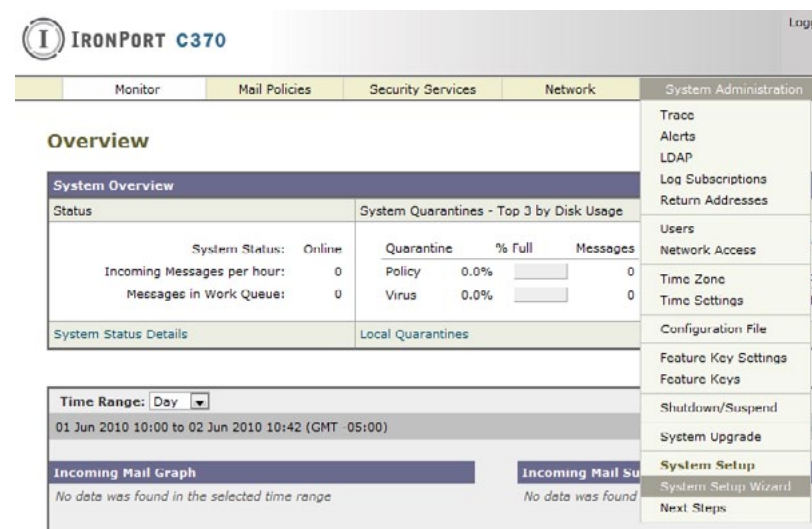
If you did not do the steps above in CLI, then to connect to the GUI device  
 manager, open a browser and browse via HTTPS to the default address of  
 the e-mail appliance (<https://192.168.42.42/>).

If you did complete the step above, then connect to the IP address config-  
 ured previously in the "Configuring Management Access" section.

### Step 4: System Setup Wizard

The next step is to run the System Setup Wizard from the GUI by connecting  
 to the IP address that was configured in the startup script from the serial  
 port connection or alternately via the 192.168.42.42 address if initial setup  
 was done by connecting to the management Ethernet interface (Figure 88).

Figure 88. System Setup Wizard



At the Start screen, read the license and click the **I accept**, then click **Begin Setup** (Not pictured).

### Step 5: System Configuration

On the System tab, enter system configuration settings like time settings and default hostname, and change the default password using the values as shown in the Figure (Figure 89).

The last two questions determine whether the ESA participates in the SenderBase network. This allows the ESA to send anonymized reputation details about email traffic back to Cisco to improve SenderBase and the product in general.

Figure 89. System Configuration

IRONPORT C370

Login Host: ironport.example.com  
Help and Support

1. Start 2. System 3. Network 4. Security 5. Review

### System Configuration

Before you enter your System and Network settings:

- Choose a configuration that best matches your network infrastructure
- Determine network and IP address assignments
- Gather information about your system setup

#### System Settings

Default System Hostname:   
example: ironport-C370.example.com

Email System Alerts To:   
example: admin@company.com

Deliver Scheduled Reports To:   
example: admin@company.com. Leave blank to only archive reports on-box.

Time Zone: Region:  Country:  Time Zone / GMT Offset:

NTP Server:

Administrator Password:   
Must be 6 or more characters.

Confirm Password:

SenderBase Network Participation: ☒ Allow IronPort to gather and report limited data on email to SenderBase in order to identify and stop email-based threats. Learn what information is shared...

AutoSupport: ☒ Send system alerts and weekly status reports to IronPort Customer Support

Cancel Next

### Step 6: Network Integration

On the Network tab, a network administrator performs network integration tasks such as setting up the network gateway and defining which interfaces to use and what DNS servers to use (or use the Internet's Root DNS servers). This tab is where the administrator needs to enter the agency's email information, what incoming mail to accept and what to do with it, and what email to relay outbound (Figure 90).

Figure 90. Network Integration

IRONPORT C370

Login Host: ironport.example.com  
Help and Support

1. Start 2. System 3. Network 4. Security 5. Review

### Network Integration

#### Network Configuration

Gateway:

DNS: ☐ Use the Internet's Root DNS Servers ☒ Use the specified DNS Servers:

DNS Server IP Address:

DNS Server IP Address:

#### Interfaces

You must configure the Management interface and 1 interface must be configured to accept mail from the Internet.

Management Data 1 Data 2 Data 3

☐ Enable Data 1 Interface  
This interface is typically configured to accept mail.

☐ Enable Data 2 Interface  
This interface is typically configured to relay mail.

☐ Enable Data 3 Interface

☒ Enable Management Interface  
This interface is typically configured for system administration.

IP Address:

Network Mask:

Fully Qualified Hostname:   
Fully qualified hostname for this appliance

Accept Incoming Mail: ☒ Accept mail on this interface

Domain:  Destination:  Add Row

example: mail.company.com or 10.1.1.1 I.e. An Exchange or Notes server

Relay Outgoing Mail: ☒ Relay mail on this interface

Mail Server:  Add Row

example: mail.company.com or 10.1.1.1

## Step 7: Message Security

On the Security tab, define message security by selecting whether antispam and antivirus filtering are enabled and which engine is used for each function (Figure 91).

Figure 91. Message Security

**Message Security**

Your IronPort appliance uses message security to protect your email infrastructure from security threats. The security solutions are applied in the order depicted below. Each module reduces the overall volume of email sent to your infrastructure.

**Anti-Spam**

SenderBase Reputation Filtering: SenderBase Reputation Filtering provides a "first line of defense" against incoming spam by restricting access to your email infrastructure based on senders' trustworthiness as determined by their SenderBase Reputation Score (SBR). More about SBR...

☒ Enable SenderBase Reputation Filtering

Anti-Spam Scanning: Select the anti-spam engine to use for the default incoming mail policy:

☐ None  
☒ IronPort Anti-Spam

☒ Enable IronPort Spam Quarantine. This setting will quarantine positive and suspect spam.

**Anti-Virus**

Anti-Virus Scanning: Select the anti-virus engine to use for the default incoming and outgoing mail policy:

☐ None  
☐ McAfee  
☒ Sophos

Virus Outbreak Filters: Virus Outbreak Filters quarantine suspicious messages even before traditional anti-virus security services have provided a signature file. More about Virus Outbreak Filters...

☒ Enable Virus Outbreak Filters

## Step 8: Finalize Initial Configuration

The Review tab (not shown here) allows review of the configuration that has been defined, and to accept or modify the configuration. If it is accepted, the ESA will install the configuration.

Click **Install this Configuration**.

Bypass the Active Directory Wizard by clicking **Cancel**.

**Tech Tip**

It is not possible to downgrade software versions, so be certain that an upgrade is desired before proceeding. It is possible that an appliance can receive different upgrade options if it is on an early release list.

## Procedure 2

## System Updates and Feature Keys

It is important to look at two other areas on the ESA before beginning to use it: feature keys and system upgrades.

### Step 1: System Updates

To upgrade the code on the appliance, select **System Administration > System Upgrade** and view the current software version. Click **Available Updates** to determine if updates are available.

If newer versions are available, they can be selected and installed. While it is not necessary to load all updates sequentially, it is possible that a later update will require interim updates before it can be loaded. If interim updates are required, the appliance will alert the operator.

Another option is to run the upgrade command from the CLI.

### Step 2: Update Feature Keys

In the web configuration tool, browse to **System Administration > Feature Keys**.

This page displays the license keys for the different features on the box. To check whether the ESA has any licenses that are not currently enabled, click **Check for New Keys**. This action will enable the ESA to connect to Cisco.com and determine if all purchased licenses are installed and enabled.

Once any new feature keys are downloaded, they can be activated.

Figure 92. Feature Keys

**Feature Keys**

Feature Keys for Serial Number: 002689363795-02NF01

| Description                    | Status | Time Remaining | Expiration Date                |
|--------------------------------|--------|----------------|--------------------------------|
| RSA Email Data Loss Prevention | Active | 1025 days      | 23 Mar 2013 22:54 (GMT -07:00) |
| Bounce Verification            | Active | Perpetual      | N/A                            |
| IronPort Email Encryption      | Active | 1025 days      | 23 Mar 2013 22:54 (GMT -07:00) |
| IronPort Anti-Spam             | Active | 1025 days      | 23 Mar 2013 22:53 (GMT -07:00) |
| Incoming Mail Handling         | Active | Perpetual      | N/A                            |
| Centralized Management         | Active | 1025 days      | 23 Mar 2013 22:53 (GMT -07:00) |
| Virus Outbreak Filters         | Active | 1025 days      | 23 Mar 2013 22:53 (GMT -07:00) |
| Sophos Anti-Virus              | Active | 1025 days      | 23 Mar 2013 22:53 (GMT -07:00) |
| McAfee                         | Active | 30 days        | 02 Jul 2010 12:55 (GMT -07:00) |

**Pending Activation**

No feature key activations are pending.

[Check for New Keys](#)

**Feature Activation**

Feature Key:

[Submit Key](#)

### Procedure 3 Setup Bounce Verification

One of the last steps of setting up a standard configuration for the ESA is setting up Bounce Verifications. Bounce verification is a process that allows the ESA to tag outgoing messages with a specific tag so that when bounced emails come back to the ESA, it can verify that the emails were actually sent out originally by the ESA. Spammers and hackers use fake bounced messages for many malicious purposes.

#### Step 1: Create Bounce Verification Key

To set up bounce verifications, select **Mail Policies > Bounce Verifications**. Click **New Key**.

Enter an arbitrary text string that the ESA will apply in the Bounce verification process. Commit the changes (Figure 93).

Figure 93. Bounce Verification

IRONPORT C370

Logged in as: admin on c370.cisco.local

Options Help and Support

Monitor Mail Policies Security Services Network System Administration

**Bounce Verification**

Success — New current key added.

**Bounce Verification Settings**

Action when invalid bounce received: Reject

Smart exceptions to tagging: Enabled

**Bounce Verification Address Tagging Keys**

New Key... Clear All Keys

| Address Tagging Keys  | Status                                                                                                                                   |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| TaggingKey12345       | Current<br>(see Mail Policies > Destination Controls to set or view destinations which have Bounce Verification Address Tagging enabled) |
| ESABounceVerification | Last used Wed Jun 02 13:03:58 2010 PDT                                                                                                   |

Purge Keys Not used in one month

#### Step 2: Set Bounce Verification Address Tagging to On

Select **Mail Policies > Destination Controls**.

Click **Default** in the first table, which is under the Domain header:

Change Bounce Verification to: **Perform Address Tagging Yes**

Submit and commit the changes.

Figure 94. Bounce Verification Enable

Bounce Verification:

Perform address tagging: ☒ No ☒ Yes

Applies only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.

### Procedure 4 Set Mail Policies to drop SPAM

#### Step 1: Change Spam Settings to Drop

The last step in setting up the ESA is reviewing the Incoming Mail Policies and changing the default setting to drop email that has been positively identified as spam.

To review mail policies, select **Mail Policies > Incoming Mail Policies**.

Currently there is one default mail policy.

#### Step 2: Select the entry under the Anti-Spam column header.

**Step 3:** Change a Positively Identified Spam result from a Quarantine action to a Drop action (Figure 95).

Submit and commit the changes.

Figure 95. Mail Policies—Anti Spam

IRONPORT C370

Monitor Mail Policies Security Services Network System Administration

**Mail Policies: Anti-Spam**

**Anti-Spam Settings**

Policy: Default

Enable Anti-Spam Scanning for This Policy: ☒ Use IronPort Anti-Spam service ☐ Disabled

**Positively-Identified Spam Settings**

Apply This Action to Message: Drop

Add Text to Subject: Drop

Advanced

Spam Quarantine Bounce custom header and message delivery.

Firewall Configuration

Process

- 1. Firewall DMZ Configuration
- 2. Firewall Address Translation (NAT/PAT) Configuration
- 3. Configure Firewall Policy for DMVPN Hub

Procedure 1 Firewall DMZ Configuration

The Firewall's DMZ (De-Militarized Zone) is a portion of the network where, typically, traffic to and from other parts of the network is tightly restricted. Agencies place network services in a DMZ for exposure to the Internet. These servers are typically not allowed to initiate connections to the 'inside' network, except for specific circumstances.

The various DMZ networks on the DMZ switch are connected to the ASAs on the ASAs' GigabitEthernet interface via a VLAN trunk. For this deployment, a separate DMZ for email will be created and the ESA will be deployed in the network on that DMZ. The DMZ-mail VLAN interface on the Cisco ASA is assigned an IP address, which is the default gateway for the DMZ-mail VLAN subnet. The DMZ switch's VLAN interface does not have an IP addresses assigned for the DMZ-mail VLAN.

Procedure Steps:

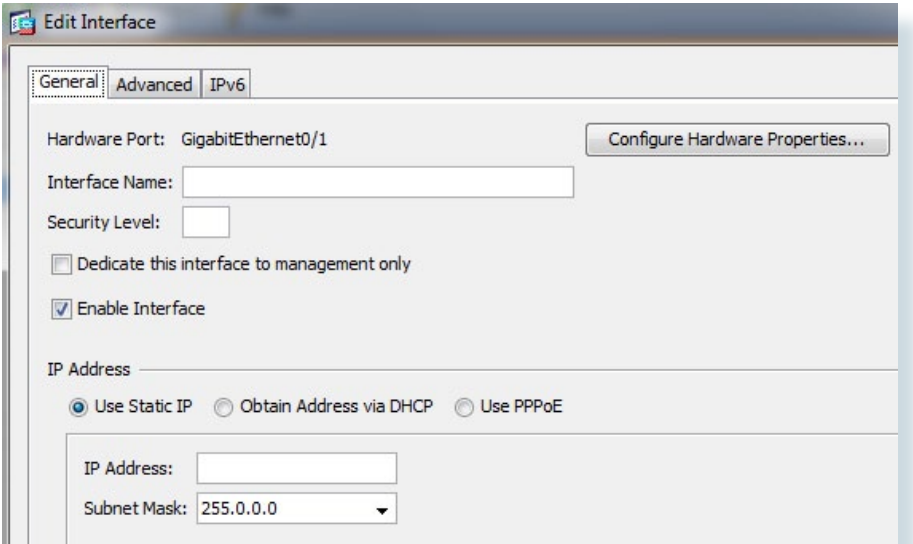
- 1. Configure ASA firewall physical interface
- 2. Configure sub-interface for DMZ-mail.
- 3. DMZ Switch Configuration

Step 1: Configure ASA firewall physical interface

**NOTE:** If there are already DMZs that have been created and configured and the ASA physical interface to the DMZ switch has already been configured, skip to Step 2.

Configure the interface that carries the VLAN trunk for the various DMZs. Values are not assigned for the interface name, security level, or IP address on trunk interfaces. Configuration details are shown in Figure 96.

Figure 96. Define DMZ Trunk Interface



```
interface GigabitEthernet0/1
description dmz trunk to dmz-3750 stack port x/0/1
no nameif
no security-level
no ip address
```

**Step 2:** Configure the DMZ VLAN connectivity on GigabitEthernet 0/1 subinterface.

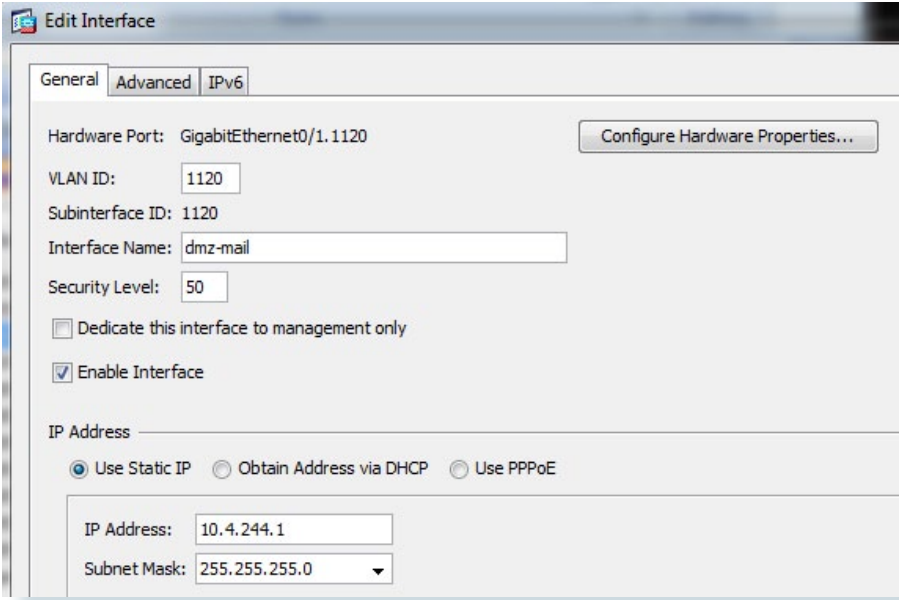
The DMZ VLAN interface must be assigned an appropriate IP address for the attached subnet, as well as an intuitive interface name to be used for NAT and security policy configuration. The tested design uses the values shown in Table 5. The configuration for one VLAN interface is displayed below (Figure 97).

Table 5. VPN-DMZ Configuration Parameters

| Interface Label         | IP Address & Netmask | VLAN | Security Level | Name     |
|-------------------------|----------------------|------|----------------|----------|
| GigabitEthernet0/1.1120 | 10.4.244.1/24        | 1120 | 50             | dmz-mail |



Figure 97. DMZ Sub-interface Configuration



```
interface GigabitEthernet0/1.1120
vlan 1120
nameif dmz-mail
security-level 50
ip address 10.4.244.1 255.255.255.0 standby 10.4.244.2
```

**Step 3:** On the DMZ switch, add the appropriate VLAN to the trunk ports that connect to the ASAs.

Use the following set of commands for primary ASA:

```
interface GigabitEthernet1/0/23
switchport trunk allowed vlan add 1120
```

And use similar commands for the standby ASA:

```
interface GigabitEthernet1/0/24
switchport trunk allowed vlan add 1120
```

Procedure 2 Address Translation Configuration

Prior to this procedure, the DMZ-mail network would have connectivity to the ASAs' interface, but there would be no access from the DMZ-mail network to the Internet, or from the Internet to the DMZ-mail. A last step is required to allow Internet connectivity for the ESA. The DMZ-mail network uses private network (RFC 1918) addressing that is not Internet routable, so the ASAs must translate the ESA address to an outside public address. For this configuration, create a static translation of the DMZ-mail address of the ESA to a public IP address that can be routed on the Internet as shown in Table 6.

Table 6. Email Security Appliance IP Address Translation Information

| DMZ Address of ESA | Outside Address of ESA on ISP-A |
|--------------------|---------------------------------|
| 10.4.244.16        | 172.16.130.16                   |

**NOTE:** As you apply the address translation configuration described in this portion of the document, the ASA will apply its default access rule set that permits traffic from higher-security interfaces to lower-security interfaces. Review your expected traffic carefully; if you cannot allow some or all traffic that is allowed by the default rules, you should shut down the various device interfaces until you have completely configured your firewall rule set.

Procedure Steps:

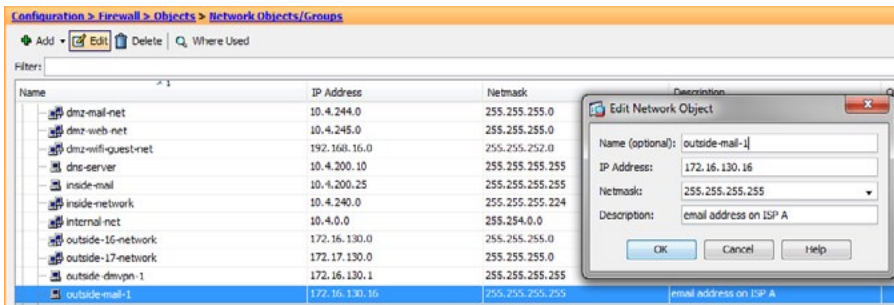
- 1. Configure name-to-address mappings for DMZ-mail subnet and ESA.
- 2. Define static translation policy for traffic passing between the Internet and the ESA in the DMZ-mail.

Step 1: Configure name-to-address mappings for DMZ-mail subnet and ESA.

These names will be used for NAT configuration, as well as Access-Rule definition. Be sure the names that you apply will be applicable for all parts of the configuration. Using address-family names and object-groups improves command-line and ASDM usability for the Cisco ASA, as the various IP networks and hosts within your agency are represented as names instead of IP addresses. Configuration of outside-mail-1 is shown in Figure 98. Repeat this for dmz-mail-net (the network information for the DMZ-MAIL network) and for DMZ-C370 (the DMZ-mail address of the C370).

Navigate to **Configuration > Firewall > Objects > Network Objects/Groups**.

Figure 98. Configure Network Object Names

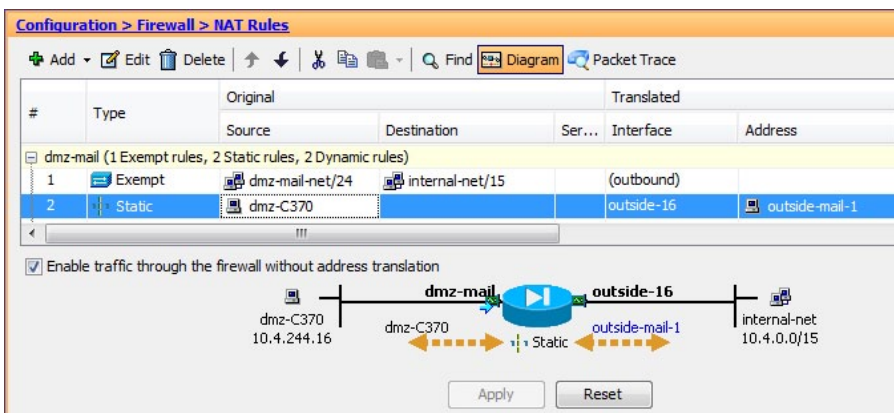


```
names
name 172.16.130.16 outside-mail-1
name 10.4.244.0 dmz-mail-net
name 10.4.244.16 dmz-C370
```

**Step 2:** Define static translation policy for traffic passing between the Internet and the ESA in the DMZ-mail.

All devices that must be exposed to the Internet will require a static translation. The ESA translation is shown in Figure 99.

Figure 99. Define Firewall Static Translation



```
static (dmz-mail,outside-16) outside-mail-1 dmz-C370 netmask
255.255.255.255
```

### Procedure 3 Configure Firewall Policy for ESA

Security policy configuration is fairly arbitrary to suit the policy and management requirements of an agency. Thus, examples here should be used as a basis for your network's security requirements.

The Email DMZ provides an additional layer of protection to lower the likelihood of certain types of misconfiguration or a compromise of a host in the DMZ exposing other devices or networks to an attacker on the Internet. A filter allows only mail traffic to the ESA. The ESA is allowed to send SMTP traffic as well as make HTTP and HTTPS connections (needed for reputation updates) to any host on the Internet. The ESA is allowed to make inbound SMTP connections to the agency exchange server as well as DNS requests to the agency's DNS server.

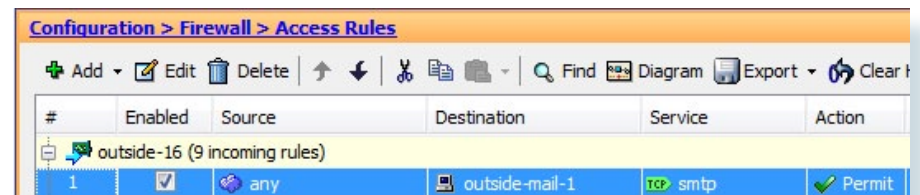
Procedure Steps:

1. Define access-control entries to allow traffic from the Internet to the ESA
2. Define access-control entries to allow ESA to access internal resources and block all other requests
3. Define access-control entries to allow internal access to ESA, but block SMTP access for all other devices

**Step 1:** Define access-control entries to allow traffic from the Internet to the ESA

This policy allows SMTP to the outside-mail-1 public address and is applied on the outside-16 interface Access Rule, and builds on existing policies (Figure 100).

Figure 100. Internet SMTP Access



**Step 2:** Define access-control entries to allow ESA to access inside and Internet resources and block other requests

This policy is applied on the DMZ-mail interface Access Rule, and builds on existing policies. It allows all devices on the dmz-mail-net to send SMTP to the inside mail host (the internal Exchange server), to make DNS requests to the dns-server host (the internal DNS server), to send logs using ssh and ftp to data center logging devices, and then block all other internal requests.

It also allows all devices on DMZ-mail to connect to any Internet host using SMTP, HTTP, and HTTPS. All other access is denied (Figure 101).

Figure 101. DMZ-Mail Access

| #                                  | Enabled                             | Source          | Destination        | Service           | Action | Description                           |
|------------------------------------|-------------------------------------|-----------------|--------------------|-------------------|--------|---------------------------------------|
| <b>dmz mail (7 incoming rules)</b> |                                     |                 |                    |                   |        |                                       |
| 1                                  | <input checked="" type="checkbox"/> | dmz-mail-net/24 | inside-mail        | smtp              | Permit |                                       |
| 2                                  | <input checked="" type="checkbox"/> | dmz-mail-net/24 | dns-server         | domain            | Permit |                                       |
| 3                                  | <input checked="" type="checkbox"/> | dmz-mail-net/24 | data-center-net/24 | ftp               | Permit |                                       |
| 4                                  | <input checked="" type="checkbox"/> | dmz-mail-net/24 | data-center-net/24 | ssh               | Permit |                                       |
| 5                                  | <input checked="" type="checkbox"/> | dmz-mail-net/24 | internal-net/15    | ip                | Deny   | Block all other traffic from mail net |
| 6                                  | <input checked="" type="checkbox"/> | dmz-mail-net/24 | any                | http, https, smtp | Permit |                                       |
| 7                                  | <input type="checkbox"/>            | any             | any                | ip                | Deny   | Implicit rule                         |

## Internet Edge 10K Deployment

Because different agencies use email in different quantities, care must be taken in sizing the appliance(s) carefully. A Cisco Partner or Account Manager can be of valuable assistance.

It is easier to deploy, manage, and maintain a single appliance, but any capacity for resilience is lost. If resilience is required, then an additional appliance can be deployed.

The Internet Edge 5K design uses a single C370 appliance that provides capacity to handle a medium message load for an agency of up to 5000 connected users, but lacks any resilience. The Internet Edge 10K design uses a pair of C370s. This provides twice the message capacity handling along with resilience.

When using the ESA in the Internet Edge 10K design, some additional steps need to be taken. Because the Internet Edge 10K design uses two ISPs and each is deployed with its own IP address space, there must be a DNS entry for the ESA for each IP address space. In the Internet Edge 10K design, the 172.16.130.0/24 range is used for ISP A and the 172.17.130.0/24 range is used for ISP B. Each ESA needs to have an address in each range and the

address needs to be mapped in DNS to the appropriate MX and A records so that if the connection to ISP A is lost, other agencies can use the MX record for ISP B so that the agency can continue reviewing mail.

To configure this functionality, an administrator will need to ensure the firewall configuration allows access to the ESA from both ISP A and ISP B. To accomplish this, a static address will need to be created for the ESA's address on the ISP B network, 172.17.130.16. In addition, access to TCP port 25 must be allowed for anyone on the Internet, which is the same access that is allowed for ISP A (Figure 102).

Figure 102. Backup ISP NAT Creation

| #                                                                 | Type   | Original        |                 | Translated |            |                |
|-------------------------------------------------------------------|--------|-----------------|-----------------|------------|------------|----------------|
|                                                                   |        | Source          | Destination     | Service    | Interface  | Address        |
| <b>dmz-mail (1 Exempt rules, 2 Static rules, 2 Dynamic rules)</b> |        |                 |                 |            |            |                |
| 1                                                                 | Exempt | dmz-mail-net/24 | internal-net/15 |            | (outbound) |                |
| 2                                                                 | Static | dmz-C370        |                 |            | outside-16 | outside-mail-1 |
| 3                                                                 | Static | dmz-C370        |                 |            | outside-17 | outside-mail-2 |

After completion, a static for the C370 ESA from dmz-mail to outside-16 and a static from dmz-mail to outside-17 should both exist and ACLs should exist to permit SMTP inbound on both outside interfaces.

For the second C370 (dmz-C370-B) used in the Internet Edge 10K design, static NAT rules must be built to both ISP-A and ISP-B and assigned an address in those address spaces (Figure 103).

Figure 103. 2nd C370 NAT Configuration

| #                                                                 | Type   | Original        |                 | Translated |            |                  |
|-------------------------------------------------------------------|--------|-----------------|-----------------|------------|------------|------------------|
|                                                                   |        | Source          | Destination     | Service    | Interface  | Address          |
| <b>dmz-mail (1 Exempt rules, 4 Static rules, 2 Dynamic rules)</b> |        |                 |                 |            |            |                  |
| 1                                                                 | Exempt | dmz-mail-net/24 | internal-net/15 |            | (outbound) |                  |
| 2                                                                 | Static | dmz-C370        |                 |            | outside-16 | outside-mail-1   |
| 3                                                                 | Static | dmz-C370        |                 |            | outside-17 | outside-mail-2   |
| 4                                                                 | Static | dmz-C370-B      |                 |            | outside-16 | outside-mail_B-1 |
| 5                                                                 | Static | dmz-C370-B      |                 |            | outside-17 | outside-mail_B-2 |

Additionally, ACLs have to be created that provide the same access as those created for dmz-C370 (Figure 104).

Figure 104. 2nd C370 ACL Configuration

| #                                                 | Enabled | Source | Destination      | Service    | Action | Description               |
|---------------------------------------------------|---------|--------|------------------|------------|--------|---------------------------|
| <b>outside-16 (11 incoming rules)</b>             |         |        |                  |            |        |                           |
| 1                                                 | ✓       | any    | outside-dmvpn-1  | 4500       | Permit |                           |
| 2                                                 | ✓       | any    | outside-dmvpn-1  | isakmp     | Permit |                           |
| 3                                                 | ✓       | any    | outside-dmvpn-1  | esp        | Permit |                           |
| 4                                                 | ✓       | any    | outside-dmvpn-1  | echo       | Permit |                           |
| 5                                                 | ✓       | any    | outside-dmvpn-1  | echo-reply | Permit |                           |
| 6                                                 | ✓       | any    | outside-mail-1   | smtp       | Permit |                           |
| 7                                                 | ✓       | any    | outside-mail_B-1 | smtp       | Permit |                           |
| 8                                                 | ✓       | any    | dmz-web-net/24   | https      | Permit |                           |
| 9                                                 | ✓       | any    | dmz-web-net/24   | http       | Permit |                           |
| 10                                                | ✓       | any    | any              | icmp       | Permit | Arshad inserted this rule |
| 11                                                |         | any    | any              | ip         | Deny   | Implicit rule             |
| <b>outside-16 IPv6 (1 implicit incoming rule)</b> |         |        |                  |            |        |                           |
| <b>outside-17 (3 incoming rules)</b>              |         |        |                  |            |        |                           |
| 1                                                 | ✓       | any    | outside-mail-2   | smtp       | Permit |                           |
| 2                                                 | ✓       | any    | outside-mail_B-2 | smtp       | Permit |                           |
| 3                                                 |         | any    | any              | ip         | Deny   | Implicit rule             |

## High Availability

The Cisco ESA functions as part of the mail transfer chain and there is a reasonable amount of resiliency built into the system since a mail server in the chain will store a message for some period of time if the destination server is unresponsive. Additional resilience is achieved by adding a second ESA. The second ESA should be configured the same as the first ESA and an additional MX record should be added to DNS.

For any additional devices, access lists and static NAT rules will need to be added to the ASA.

## Final Steps

### Monitoring

To monitor the behavior of the ESA, there are a variety of reports available under Monitor. These reports allow an administrator to track activity and statistics for spam, virus types, incoming mail domains, outbound destinations, system capacity, and system status.

## Troubleshooting

To determine why the ESA applied specific actions for a given email, an administrator can run the Trace tool under System Administration.

By defining a search using details of a given email in question, it is possible to test a specific email to determine how and why the ESA handled the message. This search capability is especially useful if some of the more advanced features of the ESA are used like DLP.

## Summary

The Cisco ESA has been configured for basic network access and an anti-spam and antivirus policy has been built and applied. DNS has been modified to support the ESA, the appliance software was updated, and the feature keys for the appliance were installed. Some slight policy changes have been made, but a detailed policy discussion, troubleshooting, and ongoing monitoring are topics that can be pursued with a Trusted Cisco Partner or account team. Policy migration and advanced policy creation for the Cisco ESA device should be directed to the local Cisco SE or partner.

## Additional Information

User documentation can be found here (login available by working with the Cisco Channel Partner): <http://www.ironport.com/support/login.html>



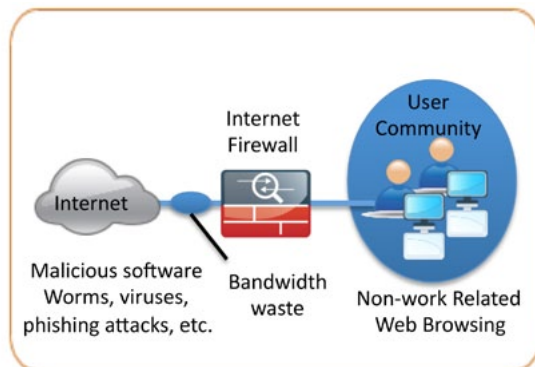
# Web Security

## Agency Overview

As access to Internet websites has moved from a nice-to-have option to a requirement in the day-to-day activity of many users, the capability for an agency to be able to protect employee productivity and manage risk by imposing agency security policy on how the users may use the web has become a requirement as well.

Another risk associated with Internet access for the agency is the pervasive threat that exists from accessing sites and content. As the monetary gain for malicious activities on the Internet has grown and developed, the methods used to affect these malicious and or illegal activities has grown and become more sophisticated. Botnets, one of the greatest threats that exists in the Internet today is that of malicious Internet servers (mostly web) being used to host content that then attacks innocent user's browsers as they view the content. These types of attacks have been used very successfully by "bot herders" to gather in millions of infected members that are subject to the whims of the people who now control their machines. Other threats include the still popular and very broad threats of viruses and trojans where a user receives a file in some manner and is tricked into running it, where the file then executes malicious code. The third variant uses directed attacks over the network. Examples of these attacks are the Internet worms that gathered so much attention in the early to mid 2000s. These types of risks are depicted below (Figure 105).

**Figure 105.** Reasons for Deploying the Web Security Appliance

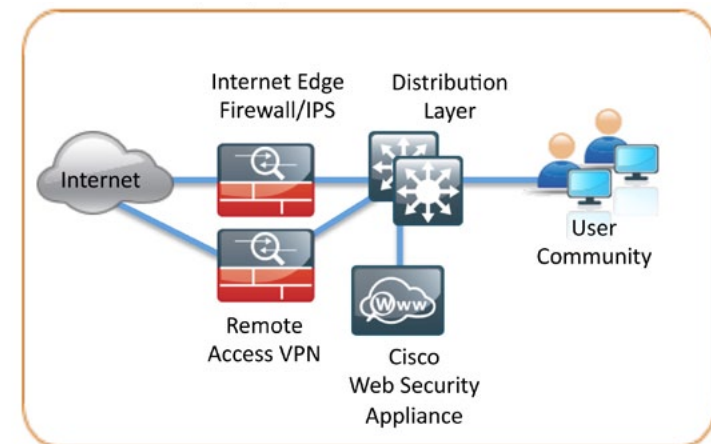


Web access is a requirement for the day-to-day functions of most agencies, but a challenge exists to maintain appropriate web access for everyone in the agency, while minimizing unacceptable or risky use. A solution is needed to control policy-based web access to ensure employees work effectively, and ensure that personal web activity will not waste bandwidth, affect productivity, or expose the agency to undue risk.

## Technical Overview

Cisco IronPort S-Series Web Security Appliance (WSA) offers a combination of web usage controls with category and reputation-based control, malware filtering, and data protection that addresses this need (Figure 106).

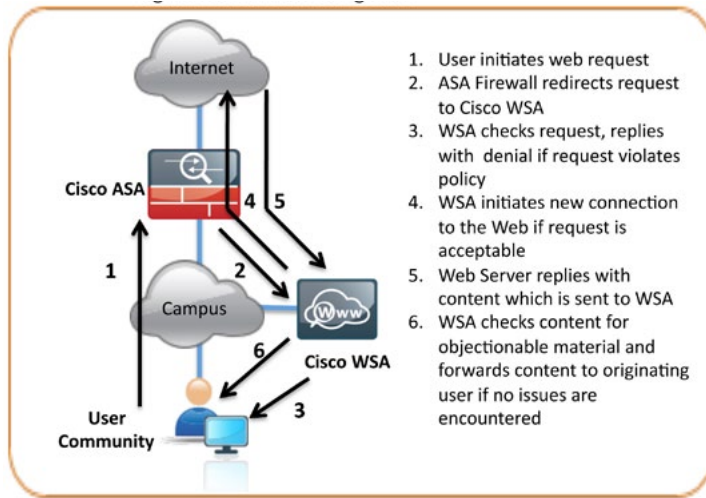
**Figure 106.** Web Security Deployment in the Borderless Network



Browsing websites can be risky and many websites inadvertently end up distributing compromised or malicious content as a result of inattention to update requirements or lax security configurations. The websites that serve the compromised and malicious content are constantly changing as human-operated and worm-infested computers scan the Internet in search of additional web servers that they can infect in order to continue propagating. This dynamic environment introduces significant challenges to maintain up-to-date Internet threat profiles.

The Cisco IronPort Web Security Appliance (WSA) Family is a web proxy that works with other Cisco network components like firewalls, routers or switches to monitor and control web content requests from within the agency and scrubs the return traffic for malicious content (Figure 107).

Figure 107. Logical Traffic Flow Using WSA



Cisco WSA is connected by one interface to the inside network of the Cisco Adaptive Security Appliance. In the Internet Edge design, the Cisco WSA connects to the same LAN switch as the ASA and on the same VLAN as the inside interface of the ASA. The Cisco ASA redirects HTTP and HTTPS connections using the Web Cache Control Protocol (WCCP) to the WSA.

Cisco WSA uses several mechanisms to apply Web Security and Content Control. The Cisco WSA begins with basic URL filtering with category-based Cisco IronPort Web Usage Controls that are based on an active database that includes analysis of sites in 190 countries in over 50 languages. Content is filtered by the reputation database. The Cisco Security Intelligence Operations updates the reputation database every five minutes. These updates contain threat information gleaned from multiple Internet-based resources, as well as content reputation information obtained from customers with Cisco security appliances that choose to participate in the Cisco SenderBase® network. If no details of the website or its content are known, the Cisco WSA applies Dynamic Content Analysis to determine the nature of the content in real time and findings are fed back to the SenderBase repository if the customer has elected to participate.

## Configuration Details

### Planning

The first step to planning the deployment of the Cisco Web Security Appliance (WSA) is to determine how web traffic will be redirected to the WSA. There are two possible methods to accomplish the redirection of traffic to the WSA: transparent proxy mode and explicit proxy mode.

In a transparent proxy deployment, all TCP traffic with a destination of port 80 or 443, is redirected to the WSA by a WCCP v2-capable network device without any configuration on the client. The transparent proxy deployment is used in this design and the Cisco ASA firewall is used to redirect traffic to the WSA because all the outbound web traffic passes through the device and is generally managed by the same technicians that will manage the WSA.

An explicit proxy deployment is when a client application, like a web browser, is configured to use an http proxy, like the WSA. From an application support standpoint, this method introduces the least amount of complications as the proxy-aware applications know about and work with the WSA directly to provide the requested content. However, from a deployment standpoint, the explicit proxy method presents challenges as to how the administrator will configure every client in the agency with the WSA proxy settings and how they will configure devices not under the agency's control. Web Proxy Automatic Detection (WPAD) and Proxy Automatic Configuration (PAC) scripts, along with tools such as Microsoft Group and System policy controls within Microsoft Active Directory (AD) make deploying this method simpler, but a discussion of those tools is beyond the scope of this document.

It is possible to use both options—explicit proxy and transparent proxy—at the same time on the same WSA. Explicit proxy is also a good way to test the configuration of the WSA as it is deployed, as explicit mode does not depend on anything else in the network to function.

The next step in planning a WSA deployment is to determine what type of physical topology will be used. The WSA has multiple interfaces and can be configured in different ways. In the Internet Edge designs, the WSA is deployed using a single interface for both proxy and management traffic.



## WSA Configuration

### Process

1. Configure Management Access
2. System Setup Wizard
3. System Update(s) and Feature Keys
4. Web Usage Controls
5. Logging
6. Custom URL Categories
7. Access Policies
8. Web Reputation and Anti-Malware
9. WCCP Configuration
10. HTTPS
11. Authentication
12. Monitoring
13. Troubleshooting

### Procedure 1 **Configure Management Access**

The first step in deploying the WSA is to complete the System Setup Wizard. This is accomplished by accessing the WSA Graphical User Interface (GUI) through a web browser.

There are two ways to reach the WSA to complete the System Setup Wizard.

1. Connect directly to the WSA with a PC and configure it via the WSA default private IP Address
2. Reconfigure the WSA IP Address via the console port prior to completing the System Setup Wizard

#### Option 1: Configure a PC to connect to the WSA private IP Address

If it is not possible to directly connect a PC to the WSA, the WSA can be reached via its default private IP address. Connect the PC Ethernet port to the WSA M1 NIC and configure the PC with an IP address in the 192.168.42.x network range (a crossover cable is not necessary for this).

The WSA IP address can also be changed using a serial out-of-band connection if the WSA needs to be connected to the agency's network to be able to reach the WSA.

#### Option 2: Reconfigure the WSA IP Address

This step is only required if the deployment model does not use a PC to connect directly to the WSA to perform the System Setup Wizard and the default IP information has to be changed to reach the WSA. To change the WSA network settings via a serial console port, connect using a standard null modem cable with the terminal emulator settings of 8-1-none 9600 baud.

**Important Consideration:** The commands that follow require a hostname to be entered. This configured hostname for the WSA needs to be fully resolvable forwards and reverse, as well as in short form within the DNS system.

```
ironport.example.com> interfaceconfig
```

Currently configured interfaces:

1. Management (192.168.42.42/24 on Management: ironport.example.com)

Choose the operation you want to perform:

- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.

```
[>]edit
```

Enter the number of the interface you wish to edit.

```
[>] 1
```

IP Address (Ex: 192.168.1.2):

```
[192.168.42.42]> 10.4.240.15
```

Netmask (Ex: "255.255.255.0" or "0xffffffff00"):

```
[255.255.255.0]> 255.255.255.224
```

Hostname:

```
[ironport.example.com]> s370.cisco.local
```

Do you want to enable FTP on this interface? [Y]>

Which port do you want to use for FTP?

```
[21]>
```

Do you want to enable SSH on this interface? [Y]>

Which port do you want to use for SSH?

```
[22]>
```

```

Do you want to enable HTTP on this interface? [Y]>
Which port do you want to use for HTTP?
[8080]>

Do you want to enable HTTPS on this interface? [Y]>
Which port do you want to use for HTTPS?
[8443]>

You have not entered an HTTPS certificate. To assure privacy,
run
"certconfig" first. You may use the demo, but this will not be
secure.
Do you really wish to use a demo certificate? [Y]>

Both HTTP and HTTPS are enabled for this interface, should
HTTP requests redirect to the secure service? [Y]>

Currently configured interfaces:
1. Management (192.168.31.240/24 on Management: websec1.cisco.
local)

Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
[]>

ironport.example.com> setgateway

Warning: setting an incorrect default gateway may cause the
current
connection to be interrupted when the changes are committed.
1. Management Default Gateway
2. Data Default Gateway
[]> 1

Enter new default gateway:
[]> 10.4.240.1

ironport.example.com> commit

```

After configuring the WSA, it should be able to ping devices on the network, assuming appropriate network access has been created (on the firewall if needed). The following output is a capture of the WSA pinging its default gateway:

```

s370.cisco.local> ping 10.4.240.1
Press Ctrl-C to stop.
PING 10.4.240.1 (10.4.240.1): 56 data bytes
64 bytes from 10.4.240.1: icmp_seq=0 ttl=255 time=0.497 ms
64 bytes from 10.4.240.1: icmp_seq=1 ttl=255 time=9.387 ms
64 bytes from 10.4.240.1: icmp_seq=2 ttl=255 time=0.491 ms
^C

```

## Procedure 2

## Complete the System Setup Wizard

Procedure Steps:

1. Accept License
2. Web Security Appliance functions
3. Network Context
4. Proxy Mode
5. Deployment Summary
6. System Settings
7. Network Interfaces and Wiring
8. Routes for Management and Data Traffic
9. Transparent Connection Settings
10. Administrative Settings
11. Security
12. Review

Access the WSA GUI by opening a browser and browsing to the WSAs IP via HTTPS on port 8443.

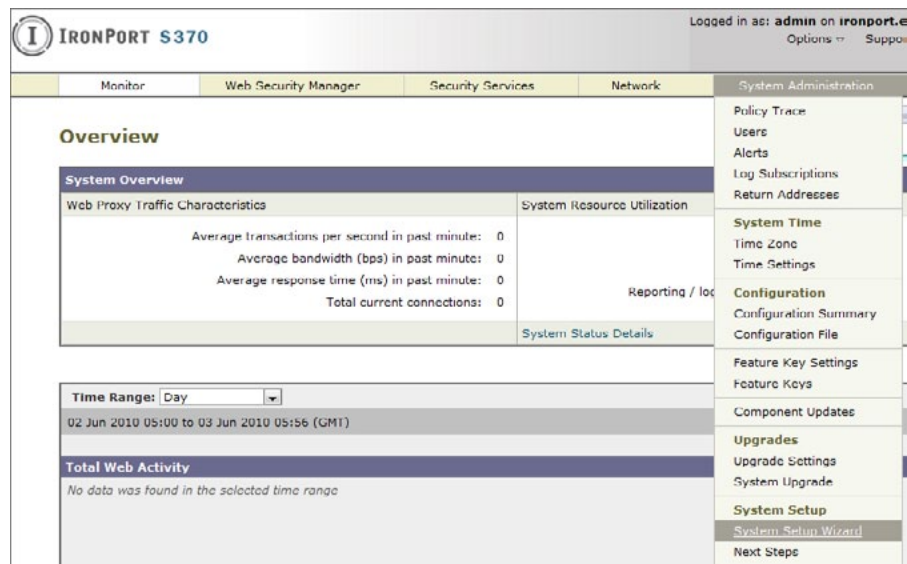
`https://[IP Address]:8443`

After logging in the wizard is accessed from **System Administration > System Setup Wizard** (Figure 108).

It is best to perform only the minimal configuration possible through the System Setup Wizard, leaving the more advanced configurations to their respective sections in the UI. In other words, configure only the basic network settings, DNS information, time settings, and username/password information as described below.

Understand that the System Setup Wizard specific screens and options vary by code version. Depending on the starting code version of the appliance being configured, the screens displayed may differ from those shown below.

Figure 108. System Setup Wizard



!

### Tech Tip

The Cisco Web Security Appliance has a default username/password of admin/ironport.

**Step 1:** On the **Start** tab, read the license and accept the terms, then click **Begin Setup** (not pictured).

**Step 2:** On the **Deployment > Web Security Appliance** functions tab, accept the defaults and click **Next** (not pictured).

**Step 3:** **Deployment > Network Context** tab.

Since the WSA is the last proxy in nearly any network deployment, this screen can be skipped. Click **Next** (not pictured).

**Step 4:** **Deployment-Proxy Mode**

The WSA will be deployed in Transparent Mode so the defaults are correct here. Click **Next** (not pictured).

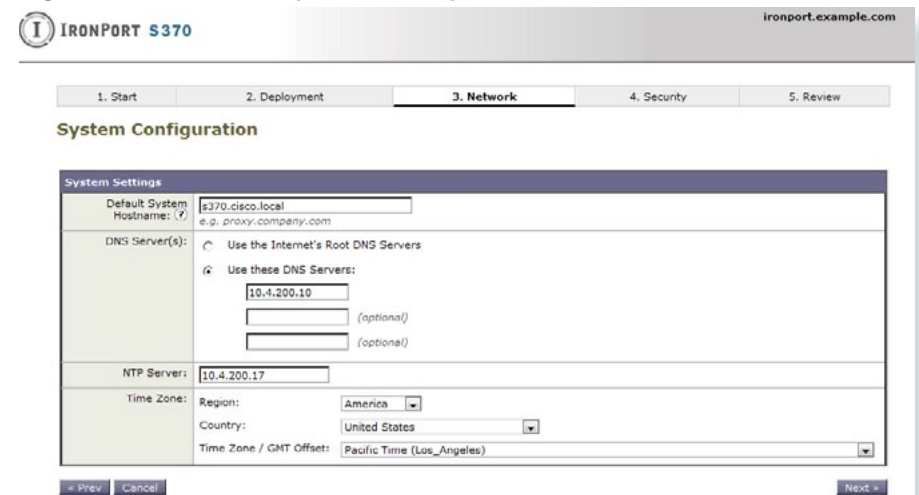
**Step 5:** **Deployment Summary**

Click **Next** to accept (not pictured).

**Step 6:** On the **Network > System Settings** tab, configure system settings.

This panel sets up the default hostname, DNS, and time. NTP is used because effective security practices require a common time reference throughout a network (Figure 109). Click **Next**.

Figure 109. Network System Settings



## Step 7: Network Interfaces and Wiring

This screen sets up which interface will be used and what IP addresses are used on each interface. In this deployment, for simplicity, M1 is used for both management and proxy services and is the only interface used. If they are not already configured, configure the IP Address, Network Mask, and host-name for the WSA. Do not check the box for **Use M1 port for Management only**. Do not use interface P1. Click **Next** (Figure 110).

Figure 110. Network Interfaces and Wiring

The screenshot shows the 'Network Interfaces and Wiring' configuration screen for an IronPort S370 appliance. The top navigation bar includes '1. Start', '2. Deployment', '3. Network', '4. Security', and '5. Review'. The main area features a diagram of the appliance with ports P1, P2, T1, T2, and M1 labeled. Below the diagram, a note states: 'Note: If the Management and Data interfaces are both configured, they must be assigned IP addresses on different subnets.' The configuration is divided into three sections: 'Management', 'Data', and 'L4 Traffic Monitor'. In the 'Management' section, 'Ethernet Port' is set to 'M1', 'IP Address' is '10.4.240.15', 'Network Mask' is '255.255.255.224', and 'Hostname' is 'e370.cisco.local'. A red 'X' is placed over the checkbox 'Use M1 port for management only'. The 'Data' section has 'Ethernet Port' set to 'P1', which is crossed out with a large red 'X'. The 'L4 Traffic Monitor' section has 'Wiring Type' set to 'Duplex TAP: T1 (In/Out)'. Navigation buttons 'Prev', 'Cancel', and 'Next' are at the bottom.

**Step 8:** The Routes for Management and Data Traffic Screen displays the current Gateway information and allows entry of any static routes that might be needed.

Enter the appliance's default gateway information now, if not completed previously. No extra routed are needed. Click **Next** (not pictured).

**Step 9:** The Transparent Connection Settings Screen is where the WCCP configuration is defined. WCCP is the protocol used to redirect traffic to the WSA from the ASA.

Skip this for now by clicking **Next** (not pictured).

## Step 10: Administrative Settings

This screen is where the admin password will be set and where system alerts will be emailed (Figure 111).

Figure 111. Administrative Settings Screen

The screenshot shows the 'Administrative Settings' configuration screen for an IronPort S370 appliance. The top navigation bar includes '1. Start', '2. Deployment', '3. Network', '4. Security', and '5. Review'. The main area contains fields for 'Administrator Password', 'Email system alerts to', 'Send Email via SMTP Relay Host (optional)', and 'AutoSupport'. The 'Administrator Password' field is set to '\*\*\*\*\*' with a note 'Must be 6 or more characters'. The 'Email system alerts to' field is set to 'admin@cisco.local'. The 'Send Email via SMTP Relay Host (optional)' field is set to 'mail.cisco.local' with a note 'e.g., smtp.example.com, 10.0.0.3'. The 'AutoSupport' section has a checkbox 'Send system alerts and weekly status reports to IronPort Customer Support' which is unchecked. Navigation buttons 'Prev', 'Cancel', and 'Next' are at the bottom.

**Step 11:** On the **Security** tab, define the security policy for the appliance and what actions will be taken for the different security features. The default configuration is fine as it leaves the appliance in Monitor mode for malware and spyware scanning.

It is also where SenderBase Network Participation is defined. This is how the administrator controls if data is fed back into Cisco SenderBase and if so, what type of data (Figure 112).

Figure 112. Security Settings

The screenshot shows the IronPort S370 configuration interface. The top navigation bar includes tabs for 1. Start, 2. Deployment, 3. Network, 4. Security (selected), and 5. Review. The main content area is titled 'Security Services' and contains several sections:

- Web Proxy:** IP Spoofing is set to ☐ Enable. A note states: 'If an upstream proxy requires client IP addresses (for IP-based authentication or access control), enable IP spoofing. If using a WCCP router, configure an additional service to redirect based on source port (return path).'.
- L4 Traffic Monitor:** Action is set to ☒ Monitor only and ☐ Block.
- URL Filtering:** IronPort URL Filtering is set to ☒ Enable. A note states: 'The Global Web Filtering Policy will be initially configured to monitor all pre-defined categories.'
- Web Reputation:** Web Reputation Filters is set to ☒ Enable. A note states: 'The Global Web Filtering Policy will be initially configured to use Web Reputation Filtering.'
- IronPort DVS™ Engine:** Malware and Spyware Scanning is set to ☒ Enable Webroot and ☒ Enable McAfee. A note states: 'The Global Web Filtering Policy will be initially configured to apply the actions configured below.'
  - Action for Detected Malware: ☒ Monitor only, ☐ Block.
  - Action for Unscannable Transactions: ☒ Monitor only, ☐ Block.
- SenderBase Network Participation:** Network Participation is set to ☒ Allow IronPort to gather anonymous statistics on HTTP requests and report them to IronPort in order to identify and stop web-based threats.
  - Participation Levels: ☒ Limited - Summary URL information, ☐ Standard - Full URL information. (Recommended).
  - A link 'Learn what information is shared...' is provided.

At the bottom, there are buttons for '< Prev', 'Cancel', and 'Next >'.

**Step 12:** Review the configuration to ensure it is correct before applying it. Then click **Install this Configuration** (not pictured).

After installation, a browser reconnect will be needed if the IP address is changed from the default. Remember that if the PC address was changed to connect to the WSA, it will be necessary to change it back to an appropriate setting in the network to reconnect to the WSA using the newly assigned IP address.



## Tech Tip

It is not possible to downgrade software versions, so be certain that an upgrade is desired before proceeding. It is possible that an appliance can receive different upgrade options if it is on an early release list.

## Procedure 3

## System Updates and Feature Keys

Procedure Steps:

1. Upgrade the appliance software
2. Install the license keys

It is important to look at two other areas on the WSA before going any further: feature keys and system upgrades. Both of these areas require the WSA to have HTTP/S Internet access.

**Step 1:** Upgrade the appliance software.

Select **System Administration > System Upgrade** to upgrade the code on the appliance. The display will show the current software version. Click **Available Updates** to see what newer updates are available.

If newer versions are available, they should be selected and installed. In general, all upgrades should be installed. Each upgrade will usually require a reboot of the appliance. The entire process can take some time.

It is also possible to upgrade from the console. Run the **upgrade** command until no new upgrades are available:

```
websec1.cisco.local> upgrade
No available upgrades.
```

This indicates that the appliance is fully upgraded.



**Step 2:** Install the license keys.

## System Administration > Feature Keys

This section is where the license keys for the different features on the box are displayed. To check to see whether the appliance has any licenses that are not currently enabled, click **Check for New Keys**. This action will instruct the WSA to make a connection to the license service and query to see if it has all the features it is allowed to run. It is very likely that after upgrading code, especially if many upgrades were applied, there will be missing feature keys. The figure below shows what an appliance feature key display might look like after being upgraded to the latest generally available version of code and then checking for updated feature keys (Figure 113).

Figure 113. Feature Keys

| Description                       | Status | Time Remaining | Expiration Date         |
|-----------------------------------|--------|----------------|-------------------------|
| IronPort Web Proxy & DVS™ Engine  | Active | Perpetual      | N/A                     |
| IronPort L4 Traffic Monitor       | Active | Perpetual      | N/A                     |
| IronPort Web Reputation Filters   | Active | 1010 days      | Sat Mar 9 15:41:00 2013 |
| Cisco IronPort Web Usage Controls | Active | 1010 days      | Sat Mar 9 15:41:17 2013 |
| IronPort URL Filtering            | Active | 1010 days      | Sat Mar 9 15:41:00 2013 |
| McAfee                            | Active | 1010 days      | Sat Mar 9 15:41:00 2013 |
| IronPort HTTPS Proxy              | Active | Perpetual      | N/A                     |
| Webroot                           | Active | 1010 days      | Sat Mar 9 15:41:00 2013 |

Note that some keys might have less than 30 days remaining, which likely indicates an Evaluation Appliance. A user-purchased box will have approximately one or more years of remaining time.

Also note that the keys include one labeled **Cisco IronPort Web Usage Controls**. This key is a feature that was added to the appliance in some of the most recent software releases. If the WSA came with an older version of code before this feature was added, it will not have a key for it initially.

If the appliance is missing keys or the duration of the keys is not correct, contact a trusted partner or Cisco reseller to resolve the issue. Have the appliance serial number available. The serial number can be found at the top of the Feature Key page.

## Procedure 4 Web Usage Controls

Enable security services on the WSA by turning on the web usage controls.

**Step 1:** Go to **Security Services > Acceptable Use Controls**.

**Step 2:** Click **Edit Global Settings**.

**Step 3:** Change the IronPort URL Filters to **Cisco Ironport Web Usage Controls**, and click **Enable Dynamic Content Analysis Engine** (Figure 114).

Figure 114. Acceptable Use Controls

**Edit Acceptable Use Controls Settings**

Acceptable Use Controls Settings

When Acceptable Use Controls service is enabled, a user could configure acceptable use policies based on URL filtering and more.

☒ **Enable Acceptable Use Controls**

Acceptable Use Controls Service: ☐ IronPort URL Filters ☒ Cisco IronPort Web Usage Controls ☐ Enable Dynamic Content Analysis Engine

Default Action for Unreachable Service: ☒ Monitor ☐ Block

Cancel Submit

**Step 4:** Submit (read and accept the license agreement if presented) and then Commit changes.

The Acceptable Use Controls main page lists the Acceptable Use Controls Engine Updates. Click **Update Now** and wait until the page reports back success. Ensure that at least some of the controls have an update that is current or very nearly so. Due to randomness of update schedules, it is impossible to know when updates will come out for each component. The Web Categories Prefix Filters and the Web Categories List get updated fairly often and are good bets for recent update histories (Figure 115).



Figure 115. Engine Updates

IronPort S370

Logged in as: admin on s370.cisco.local  
Options Support and Help

Monitor Web Security Manager Security Services Network System Administration

Acceptable Use Controls

Success — Component updates requested.

Acceptable Use Controls Settings

|                                         |                                   |
|-----------------------------------------|-----------------------------------|
| Acceptable Use Controls Service Status: | Enabled                           |
| Active Acceptable Use Controls Engine:  | Cisco IronPort Web Usage Controls |
| Dynamic Content Analysis Engine:        | Disabled                          |
| Default action for Unreachable Service: | Monitor                           |

Edit Global Settings...

Acceptable Use Controls Engine Updates

| File Type                                                                  | Last Update             | Current Version |
|----------------------------------------------------------------------------|-------------------------|-----------------|
| IronPort URL Filtering Engine                                              | Never Updated           | 5.2.2           |
| IronPort URL Categories Database                                           | Thu Jun 3 00:39:39 2010 | 2523            |
| IronPort URL Categories Database Incremental Updates                       | Thu Jun 3 00:39:39 2010 | 2552            |
| Cisco IronPort Web Usage Controls - Web Categorization Engine              | Thu Jun 3 00:38:56 2010 | 2.1.0.101       |
| Cisco IronPort Web Usage Controls - Web Categorization URL Keyword Filters | Thu Jun 3 00:45:01 2010 | 1265751908      |
| Cisco IronPort Web Usage Controls - Web Categorization Prefix Filters      | Thu Jun 3 12:04:26 2010 | 1275591207      |
| Cisco IronPort Web Usage Controls - Web Categorization Categories List     | Thu Jun 3 00:45:01 2010 | 1275527942      |
| Cisco IronPort Web Usage Controls - Dynamic Content Analysis Engine        | Never Updated           | 2.0.0-025       |
| Cisco IronPort Web Usage Controls - Dynamic Content Analysis Engine Data   | Thu Jun 3 12:03:44 2010 | 290004          |

Update Now...

The WSA can now be tested for functionality. We do this by setting up a client on the inside of the network with the WSA as the explicit proxy in the web browser of their choice. Use the IP address of the WSA as the proxy and set the port to 3128.

Test two different addresses. One address should be resolvable externally, for instance [www.cisco.com](http://www.cisco.com), which should return without issue. This proves the client has Internet access, but does not prove the connection is going through the WSA. The other address should be something not resolvable externally. This request should return an error from the WSA, not the browser; proving the WSA is serving the content.

Firefox returns an error like that shown in Figure 116:

Figure 116. Browser Error

**Server not found**

Firefox can't find the server at [www.bob.bob](http://www.bob.bob).

- Check the address for typing errors such as [ww.example.com](http://ww.example.com) instead of [www.example.com](http://www.example.com)
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Try Again

The WSA returns an error like that shown in Figure 117:

Figure 117. WSA Error

### This Page Cannot Be Displayed

The host name resolution (DNS lookup) for this host name ( bob.cisco.local ) has failed. The Internet address may be misspelled or obsolete, the host ( bob.cisco.local ) may be temporarily unavailable, or the DNS server may be unresponsive.

Please check the spelling of the Internet address entered. If it is correct, try this request later.

If you have questions, or if this condition persists, please contact your corporate network administrator and provide the codes shown below.

Notification codes: (1, DNS\_FAIL, bob.cisco.local)

## Procedure 5

### Enable Logging

Procedure Steps:

1. Add Log Subscription
2. Submit and Commit

To monitor Web Usage, the appliance stores client access data for a relatively short duration, and rotates logs for space reasons. For users looking for long-term compliance reporting, they should look into the Cisco software solution called Sawmill for IronPort. This software is either an add-on for the larger installations or comes bundled in the package for smaller purchases. This guide does not cover the installation or use of the Sawmill product.

For the Sawmill reporting product to work, the WSA needs to send its logs over to an FTP server where the Sawmill product can access them. For this deployment, it is assumed an FTP server is already deployed and configured. The following configuration moves the log access logs off the WSA to the FTP server (Figure 118).

**Step 1: System Administration > Log Subscriptions** and click **Add Log Subscription**.

Add the new logging information (Figure 118).

**Figure 118.** Log Subscriptions

**Step 2: Click Submit and then Commit changes.**

Figure 119 shows the results after inputting the changes:

**Figure 119.** Configured Subscriptions

| Configured Log Subscriptions |             |                                   |                          |        |
|------------------------------|-------------|-----------------------------------|--------------------------|--------|
| Add Log Subscription...      |             |                                   |                          |        |
| Log Name                     | Type        | Log Files                         | All Rollover             | Delete |
| Accesslogs                   | Access Logs | ftp://10.4.200.10/EmailAccesslogs | <input type="checkbox"/> |        |

## Procedure 6 Custom URL Categories

Procedure Steps:

1. Add Custom Categories
2. Create Block List
3. Monitor, Warn and Allow Lists
4. Submit and Commit

The next configuration step for the WSA is to set up standard custom URL categories that most administrators find they need to implement for their desired URL filtering.

**Step 1: Select Web Security Manager > Custom URL Categories** and click **Add Custom Category**.

**Step 2: Add four placeholders for the four different action exceptions where we can put URLs. Create four different Custom URL Categories. The title of the first one is "Block List" (Figure 120).**

**Figure 120.** Adding custom category

### Custom URL Categories: Add Category

A placeholder URL (block.com) has to be entered because it is not possible to create a category and have it be empty. In the future, when a URL is found that needs to be blocked, add it to the list, and then delete the placeholder. Submit.

**Step 3: Now create three more lists using these three titles: "Monitor List", "Warn List", and "Allow List" following the template above.**

This will create an ordered list of custom categories (Figure 121).

Figure 121. Custom Categories

Custom URL Categories

Success — The Custom URL Category "Allow List" was added

Custom URL Categories

Add Custom Category...

| Order | Category     |
|-------|--------------|
| 1     | Block List   |
| 2     | Monitor List |
| 3     | Warn List    |
| 4     | Allow List   |

Step 4: Commit the changes.

Procedure 7

Access Policies

Procedure Steps:

1. Access Policies
2. Include each Custom URL
3. Change the Actions for each Category
4. Web Acceptable Use Configuration
5. Submit and Commit

Now that we have created the Custom Categories, we need to enable them for use and define actions for each.

Step 1: Select **Web Security Manager > Access Policies** and click the link beneath the **URL Categories** header (Figure 122).

Figure 122. Custom Category Actions

IRONPORT S370

Logged in as: admin on s370.cisco.local

Options Support and Help

MonitorWeb Security ManagerSecurity ServicesNetworkSystem Administration

No Changes Pending

Access Policies

Policies

Add Policy...

| Order | Group         | Applications  | URL Categories                                                                 | Objects                                                       | Web Reputation and Anti-Malware Filtering | Delete |
|-------|---------------|---------------|--------------------------------------------------------------------------------|---------------------------------------------------------------|-------------------------------------------|--------|
|       | Global Policy | Identity: All | Redirect: 0<br>Allow: 0<br>Monitor: 66<br>Warn: 0<br>Block: 0<br>Time-Based: 0 | HTTP/HTTPS Object Max Size: None<br>FTP Object Max Size: None | (enabled)                                 |        |

Step 2: Click **Include** for each Custom URL category (Figure 123).

Figure 123. Select Custom Categories

Access Policies: URL Categories: Global Policy

Custom URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

|                                                 | Redirect   | Allow      | Monitor    | Warn       | Block      | Time-Based    |
|-------------------------------------------------|------------|------------|------------|------------|------------|---------------|
|                                                 | Select all | Select all | Select all | Select all | Select all | (Unavailable) |
| View: Included Categories Only   All Categories |            |            |            |            |            |               |
| Block List                                      | [Exclude]  |            |            | ✓          |            | —             |
| Monitor List                                    | [Exclude]  |            |            | ✓          |            | —             |
| Warn List                                       | [Exclude]  |            |            | ✓          |            | —             |
| Allow List                                      | [Include]  |            |            |            |            | —             |

Step 3: On the **Access Policies** page, change the action of the Custom Category to match the category name. For example, change **Block List** to have the **Block** action, **Monitor List** to the **Monitor** action, and so on (Figure 124). Click **Submit**.

Figure 124. Changing Custom Category Actions

Access Policies: URL Categories: Global Policy

Custom URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

|                                                 | Redirect   | Allow      | Monitor    | Warn       | Block      |
|-------------------------------------------------|------------|------------|------------|------------|------------|
|                                                 | Select all | Select all | Select all | Select all | Select all |
| View: Included Categories Only   All Categories |            |            |            |            |            |
| Block List                                      | [Exclude]  |            |            |            | ✓          |
| Monitor List                                    | [Exclude]  |            | ✓          |            |            |
| Warn List                                       | [Exclude]  |            |            | ✓          |            |
| Allow List                                      | [Exclude]  | ✓          |            |            |            |

**Step 4:** On this page, the agency's web acceptable use policy can also be implemented.

This policy can include the category of the URL (adult, sports, streaming media) as well as the actions desired (monitor, warn, or block) and whether a time-based factor is involved as well.

For testing purposes, we want to change one of the predefined categories below to Block to test the deployment.

Change **Gambling** from **Monitor** to **Block** and change **Sports** from **Monitor** to **Warn** (Figure 125).

Figure 125. URL Category Actions

| Predefined URL Category Filtering                                                                                       |            |            |            |
|-------------------------------------------------------------------------------------------------------------------------|------------|------------|------------|
| These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy. |            |            |            |
| Category                                                                                                                | Monitor    | Warn       | Block      |
|                                                                                                                         |            |            |            |
| Gambling                                                                                                                | Select all | Select all | Select all |

**Step 5:** Submit and commit all changes.

To test these changes using a browser explicitly pointing to the WSA Appliance, try browsing to a well known gambling site.

The WSA should return the message shown in Figure 126:

Figure 126. Blocked Website

| This Page Cannot Be Displayed                                                                                                                                                                                                                                                       |  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| Based on your corporate access policies, access to this web site ( http://www. [REDACTED].com/ ) has been blocked because the web category "Gambling" is not allowed. If you have questions, please contact your corporate network administrator and provide the codes shown below. |  |
| Notification codes: (1. WEBCAT, BLOCK-WEBCAT, 0x0000062a, 1265572921.083, AAAEGOMAAAAAAAAA1v0AEP0AAAABAAAAAAAAAAQ**, http://www. [REDACTED].com/)                                                                                                                                   |  |

Procedure 8

Web Reputation and Anti-Malware

Procedure Steps:

1. Access Policies
2. Web Reputation Configuration

**Step 1:** To make changes to the Web Reputation and Malware settings, navigate to **Web Security Manager > Access Policies**.

**Step 2:** Click the link underneath the **Web Reputation and Anti Malware Filtering** header (Figure 127).

Figure 127. Web Reputation

| Access Policies |               |                                                                        |                                                                                |                                                               |                                           |
|-----------------|---------------|------------------------------------------------------------------------|--------------------------------------------------------------------------------|---------------------------------------------------------------|-------------------------------------------|
| Policies        |               |                                                                        |                                                                                |                                                               |                                           |
| Add Policy...   |               |                                                                        |                                                                                |                                                               |                                           |
| Order           | Group         | Applications                                                           | URL Categories                                                                 | Objects                                                       | Web Reputation and Anti-Malware Filtering |
|                 | Global Policy | Allow: FTP over HTTP, HTTP, HTTPS, Nbtv FTP<br>Allow: Ports 20, 21,... | Redirect: 0<br>Allow: 1<br>Monitor: 64<br>Warn: 2<br>Block: 3<br>Time-Based: 0 | HTTP/HTTPS Object Max Size: None<br>FTP Object Max Size: None | (enabled)                                 |

Reputation can range from -10 as the worst to +10 being completely trustworthy. By default, websites having a -6 or worse reputation are automatically blocked, which prevents possibly infected content from being brought back into the network from such sites. Sites with reputations between -5.9 and +5.9 trigger the WSA to scan the client request and the server response using the Cisco IronPort DVS Engine. This scan looks for many possible types of attacks like phishing, malware, viruses, and worms. By default, the security policy is not set up to block these if detected. The page shown in Figure 128 is where those changes would be implemented if the agency's security policy requires it. URLs with a reputation score higher than 6.0 are passed without scanning by default.

Figure 128. Web Reputation and Anti-Malware Settings

| IRONPORT S370                                                                                                                                                                                                                                                                         |                                                                                                                          |                                                         |         |                       |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|---------|-----------------------|
| Logged in as: admin on s370.cisco.local                                                                                                                                                                                                                                               |                                                                                                                          |                                                         |         |                       |
| Options Support and Help                                                                                                                                                                                                                                                              |                                                                                                                          |                                                         |         |                       |
| Monitor                                                                                                                                                                                                                                                                               | Web Security Manager                                                                                                     | Security Services                                       | Network | System Administration |
| No Changes Pending                                                                                                                                                                                                                                                                    |                                                                                                                          |                                                         |         |                       |
| Access Policies: Reputation and Anti-Malware Settings: Global Policy                                                                                                                                                                                                                  |                                                                                                                          |                                                         |         |                       |
| Web Reputation Settings                                                                                                                                                                                                                                                               |                                                                                                                          |                                                         |         |                       |
| Enable Web Reputation Filtering                                                                                                                                                                                                                                                       |                                                                                                                          |                                                         |         |                       |
| <div>Web Reputation Score</div> <div><div>BLOCK-10.0 to -6.0</div><div>SCAN-5.9 to 5.9</div><div>ALLOW6.0 to 10.0</div></div> <div><div>-10</div><div>-8</div><div>-6</div><div>-4</div><div>-2</div><div>0</div><div>2</div><div>4</div><div>6</div><div>8</div><div>+10</div></div> |                                                                                                                          |                                                         |         |                       |
| Block                                                                                                                                                                                                                                                                                 | Scan                                                                                                                     | Allow                                                   |         |                       |
| The requested URL is immediately blocked.                                                                                                                                                                                                                                             | The IronPort DVS™ engine scans the client request and the server response.<br>Note: Sites with no score will be scanned. | The requested URL is allowed. No scanning is performed. |         |                       |

## Procedure 9

## Configuring WCCP on the WSA

### Procedure Steps:

1. Transparent Redirection: Edit Device
2. Select WCCP v2 Router
3. Submit
4. Add Service
5. Commit Changes

Now that we have the WSA working and applying an access policy for HTTP traffic, we can implement the Web Cache Communications Protocol (WCCP) on the WSA and the ASA firewall. Implement WCCP allows the WSA to begin to receive traffic directly from the ASA instead of having browsers configured to use the WSA as an explicit proxy.

To configure WCCP on the **WSA**, click **Network > Transparent Redirection**.

**Step 1:** Select **Edit Device** to add a new redirect device.

**Step 2:** From the **Type** pull down menu select **WCCP v2 Router**.

**Step 3:** Click **Submit**.

**Step 4:** Click **Add Service** under WCCPv2 Services

This is where we will define the policy that the Internet Edge ASA will use to redirect traffic to the WSA. It pulls the policy off the WSA using the name of the policy as defined on the WSA.

The Service Profile Name names this policy: **HTTP\_and\_HTTPS\_WCCP**

The Dynamic service ID is the number used to define this policy and is the ID used by ASA to request the policy: **90**

In this policy, redirect ports are HTTP and HTTPS: **80, 443**

The Router IP address is the inside address of the ASA: **10.4.240.30** (Figure 129)

Figure 129. HTTP and HTTPS WCCP

WCCP v2 Service

Service Profile Name: **HTTP\_and\_HTTPS\_WCCP**

Service: ☐ Standard service ID: 0 web-cache (destination port 80)  
(Not available, already defined)

☒ Dynamic service ID: **90** 0-255

Port numbers: **80,443**  
(up to 8 port numbers, separated by commas)

☒ Redirect based on destination port

☐ Redirect based on source port (return path)

*For IP spoofing, define two services, one based on port and another based on source port (return path).*

☒ Load balance based on server address

☐ Load balance based on client address

*Applies only if more than one Web Security*

Router IP Addresses: **10.4.240.30**

Separate multiple entries with line breaks or commas.

Service Profile Name: **Standard\_HTTP\_Only\_WCCP**



### Tech Tip

HTTPS proxy has not yet been set up on the WSA, so if WCCP redirect were to be initiated for HTTPS immediately, those connections would fail until it gets configured. If the WSA/ASA deployment is live and operational and cannot have downtime, create an additional policy for just port 80 temporarily (Figure 130). After configuring the HTTPS policy on the WSA, change the policy used on ASA to instead pull the HTTP and HTTPS policy.

Dynamic Service ID: **0 (web\_cache)**

Ports: **80**

Router IP Address: **10.4.240.40**



Figure 130. Standard HTTP Only WCCP

WCCP v2 Service

Service Profile Name:

Service:

☒ Standard service ID: 0 web-cache (destination port 80)

☐ Dynamic service ID: -255

Port numbers:

(up to 8 port numbers, separated by commas)

☒ Redirect based on destination port

☐ Redirect based on source port (return port)

For IP spoofing, define two services, one based on source port and another based on source port (return port)

☐ Load balance based on server address

☐ Load balance based on client address

Applies only if more than one Web Security Service is configured

Router IP Addresses:

Separate multiple entries with line breaks or commas.

The WCCP services panel should look like the below figure after completion (Figure 131).

Figure 131. WCCPv2 Services

IRONPORT S370

Logged in as: admin on s370.cisco.local

Options Support and Help

Monitor Web Security Manager Security Services Network System Administration

No Changes Pending

**Transparent Redirection**

Transparent Redirection Device

Type: WCCP v2 Router

Edit Device...

WCCP v2 Services

Add Service...

| Service Profile Name | Service ID    | Router IP Addresses | Ports  | Delete |
|----------------------|---------------|---------------------|--------|--------|
| Standard_Web_Only    | 0 (web-cache) | 10.4.240.30         | 80     |        |
| HTTP_and_HTTPS_WCCP  | 90            | 10.4.240.30         | 80,443 |        |

Step 5: Commit all changes.

## Procedure 10 Configuring WCCP on the Firewall

Procedure Steps:

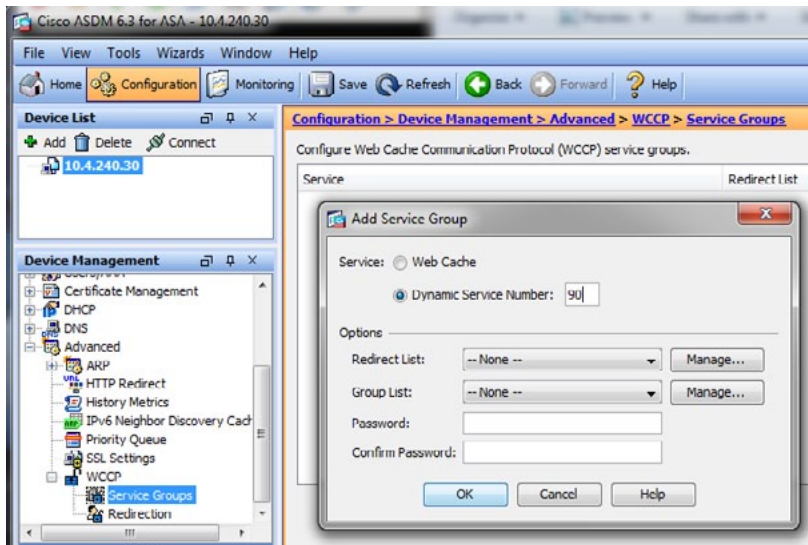
1. ASDM WCCP Configuration
2. Service Groups
3. Redirect Lists
4. Add ACL
5. Add ACE
6. Add ACE
7. Apply the Redirect ACL
8. Add WCCP Redirection
9. Test a Resolvable Address
10. Test a Blocked Address
11. Check ASA to Show WCCP is Working

**Step 1:** To configure the ASA firewall on the Internet Edge to redirect HTTP and HTTPS traffic to the WSA, bring up ASDM on the firewall and go to **Configuration > Device Management > Advanced > WCCP**.



**Step 2:** Under Service Groups, build a new service group using the Dynamic Service Number of 90 (or use the web\_cache for port 80 redirect only) that we defined on the WSA (Figure 132).

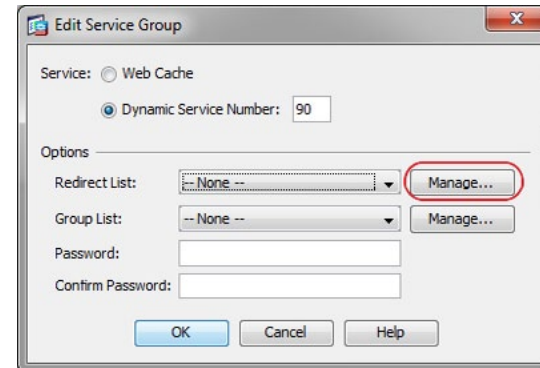
Figure 132. Configure WCCP Redirect on the ASA Firewall



The WCCP policy configured redirects all HTTP and HTTPS traffic to the WSA. This includes any traffic from the inside network to the DMZ web servers and any device management traffic that uses HTTP or HTTPS. There is little reason to send any of this traffic to the WSA. To avoid having any of this traffic redirected to the WSA, create an ACL on the firewall to filter out any HTTP or HTTPS traffic destined to RFC 1918 addresses from being redirected.

**Step 3:** In the same **Add Service Groups** window from above, click the **Manage** button to the right of the Redirect List field (Figure 133).

Figure 133. WCCP Redirect List Management

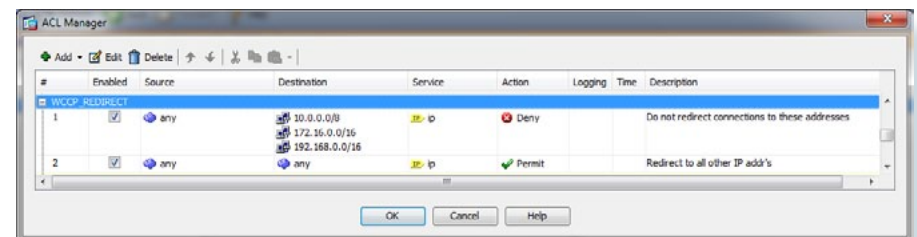


**Step 4:** In the **ACL Manager** window, select the **Add** button, and select the **Add ACL** option. Input a name for the ACL: **WCCP\_Redirect**

**Step 5:** Select the **Add ACE** button and add a line to Deny any source to all RFC 1918 addresses as the destination with a Service of IP.

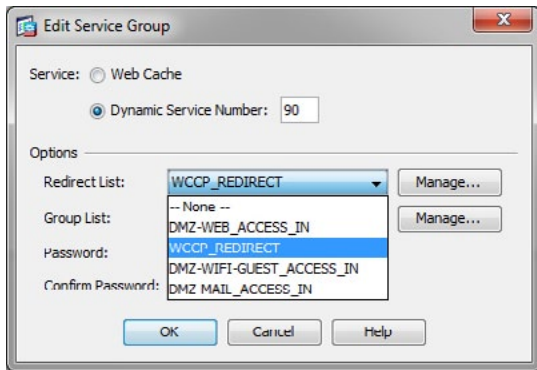
**Step 6:** Select the **Add ACE** button and add a line to Permit any source to any destination with a Service of IP. Click the **OK** button

Figure 134. Creating a WCCP Redirect ACL



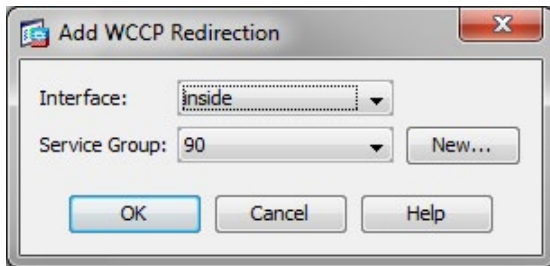
**Step 7:** On the **Add Service Group** window, in the pull down for the **Redirect List**, select the ACL created above (WCCP\_Redirect). Click the **OK** button and Apply (Figure 135).

Figure 135. Redirect List Selection



**Step 8:** Configuration > Device Management > Advanced > WCCP > Redirection on ASDM, create a policy to add the redirect for the Inside Interface using service group 90 (Figure 136).

Figure 136. Enabling the WCCP Policy on the ASA Inside Interface



To test the configuration, use a browser that is not already configured to go to the appliance as an explicit proxy (or remove the explicit proxy settings).

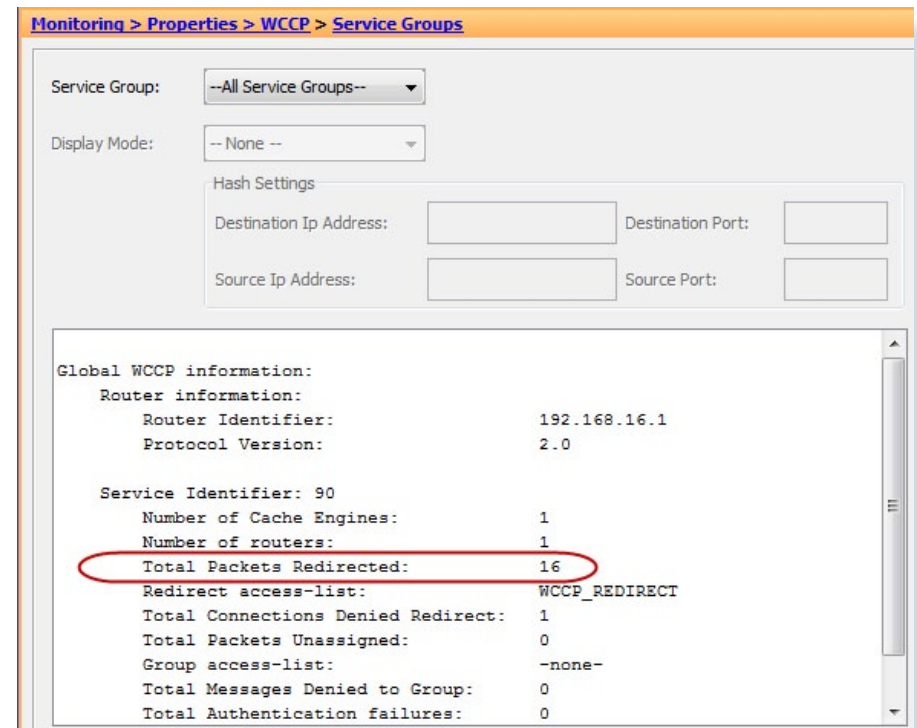
**Step 9:** Test to a resolvable allowed address like [www.cisco.com](http://www.cisco.com).

**Step 10:** Test to a resolvable blocked address (from one of the previously configured Blocked categories)

**Step 11:** To check that WCCP redirection is working, in ASDM, navigate to **Monitoring > Properties > WCCP > Service Groups**.

The status window should show a router ID that is one of the IP addresses of the ASA (in this case 192.168.16.1) and the number of cache engines is 1, which is the Cisco WSA appliance. If things are working correctly and redirections are occurring, the Total Packets Redirected counter will be increasing (Figure 137).

Figure 137. Checking that ASA Redirection is working on the ASA



## High Availability and Resilience

For availability purposes, if the WSA fails, the WCCP protocol reports that fact to the ASA and it stops redirecting traffic to the WSA by default. If web security resilience is a requirement, two or more WSAs can be deployed. To deploy multiple devices, define multiple WCCP routers on the ASA and the WCCP protocol will load balance between them. If one is down, the ASA takes that device out of the list until it comes back online and starts responding to WCCP requests again.

# HTTPS Proxy Configuration

Procedure 11

HTTPS Proxy Setup

Procedure Steps:

- 1. HTTPS Proxy Settings
- 2. Submit and Commit
- 3. Custom URL Categories
- 4. Create 3 Custom Categories
- 5. Decryption Policies
- 6. URL Categories
- 7. Change Custom URL Categories Actions

To set up the WSA to proxy HTTPS connections, start by enabling the feature.

**Step 1: Security Services > HTTPS Proxy** and then click **Enable** and **Edit Settings**.

On this page, define the ports to proxy HTTPS where the default is only on TCP 443.

A certificate for the WSA to use on the client side of the proxy connection needs to be generated. Generating a certificate typically means that the client browser will complain about the certificate for each connection to an HTTPS website. To avoid this, upload a certificate that is trusted in the agency and its matching private key file to the appliance. If the clients already have this certificate loaded on their machines, the HTTPS proxy will not generate errors related to Unknown Certificate Authority.

Besides adding an agency root certificate to the WSA, another option is to inform users in the agency to accept the root certificate supplied by the WSA as a trusted source.

For more information about using certificates as part of the WSA HTTPS Proxy mechanism, see the WSA User Guide, or consult a trusted partner or Cisco Sales Representative.

Also on the WSA HTTPS Proxy Settings page, it is possible to define the action WSA should take when it encounters an invalid certificate on an HTTPS server. The choices, depending on the certificate error, can range from dropping the connection, decrypting it, or monitoring it (Figure 138).

Figure 138. Edit HTTPS Proxy Settings

**Step 2:** After defining the policy, Click **Submit** and then **Commit** (Figure 139).

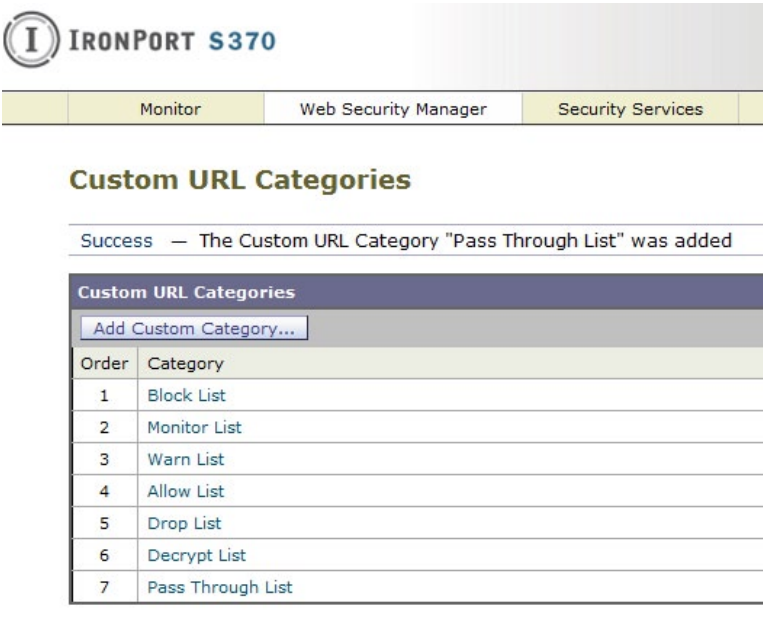
Figure 139. HTTPS Proxy Settings

The second step for HTTPS proxy configuration is to configure policies for the HTTPS proxy.

Step 3: Select Web Security Manager > Custom URL Categories.

Step 4: As before, add three new Custom Categories (make sure to include a dummy URL for each): Drop List, Decrypt List, Pass Through List (Figure 140). Commit the changes.

Figure 140. HTTPS Custom Categories

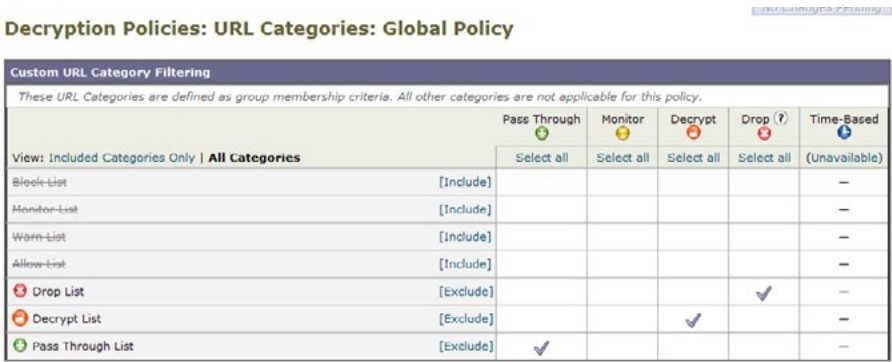


Step 5: Select Web Security Manager > Decryption Policies.

Step 6: Select the link below the URL Categories header to get to the Decryption Policies: URL Categories: Global Policy screen.

This will list all the custom categories that have been created. Do not include the ones previously created for HTTP. Only include the three new ones. Change the action of the category to correspond with their name: for example, Drop should be the action for the Drop List category (Figure 141).

Figure 141. Decryption Policies- URL Categories



The Predefined URL Categories at the bottom of the page allow an administrator to create and enforce a policy around how the WSA handles specific types of websites with relation to decryption. Some agencies have strict policies about not decrypting healthcare or financial websites and potentially other categories as well. The categories on this page allow an administrator to enforce that policy on the WSA. For example, it is possible to configure the WSA so that Financial HTTPS websites are set to Pass Through so they will not be proxied, while Gambling sites are set to Drop.

Step 7: Change Gambling to Drop, and change Finance to Pass Through (Figure 142).

Figure 142. Predefined URL Category Filtering



To test the new configuration, set up categories for webpages that you know are encrypted (HTTPS) and then use those URLs in the testing process. Because the administrator has to know whether the site uses HTTPS or not, it is easier to use Custom Categories for a specific webpage that he knows uses HTTPS and put the address into the Drop List. When that site is accessed, the WSA should drop the connection.

## Authentication Using WSA

### Procedure 12 Authentication

Procedure Steps:

1. Add Realm
2. Specify Active Directory Information
3. Join Domain
4. Test Authentication Realm Settings
5. Identities
6. Create Identities
7. Subnets not to Authenticate
8. User Agents not to Authenticate
9. Global Identity Policy
10. Changing to Authenticate as the Default
11. Submit and Commit

Authentication is the act of confirming the identity of a user. When authentication is enabled, the WSA authenticates clients on the network before allowing them to connect to a destination server. When using authentication in the WSA, it is possible to set up different web access policies by user or group membership using a central user directory. Another primary driver for using authentication is that of user tracking, so that when a user violates an acceptable use policy, the WSA can match up the user with the violation instead of just using an IP address. The last reason for authentication of web sessions is for compliance reporting.

The WSA supports two different authentication protocols: lightweight directory access protocol (LDAP) and NT LAN Manager (NTLM). Since most agencies will have an Active Directory server, they will be using NTLM. Single Sign-On (SSO) is also only available when using NTLM.

When the WSA is deployed in transparent mode with authentication enabled and a transaction requires authentication, the WSA replies to the client application asking for authentication credentials. However, not all client applications support authentication, so they have no way to prompt users to provide their usernames and passwords. These applications might have issues when the WSA is deployed in transparent mode because the application tries to run non-HTTP traffic over port 80 and cannot handle an attempt by the WSA to authenticate the connection.

Here is a partial list of applications (and these are subject to change as newer code versions are released) that do not support authentication:

- Mozilla Thunderbird
- Adobe Acrobat Updates
- Microsoft Windows Update
- Outlook Exchange (when trying to retrieve Internet-based pictures for email messages)

---

**NOTE:** If applications need to access a particular URL, then it is possible to create an identity based on a custom User Agent category that does not require authentication. When this happens, the client application is not asked for authentication.

---



For agencies that require authentication, consult a trusted Cisco IronPort Partner or Reseller or your Cisco account team. They will be able to assist in setting up an authentication solution that meets the agency's requirements, while minimizing any possible complications.

The first step in setting up Authentication is to build an Authentication Realm. A Realm defines how Authentication is supposed to occur.

In this deployment, a Realm was built for NTLM authentication to the AD server.

**Step 1:** Select **Network > Authentication > Add Realm**.

**Step 2:** In the Realm definition, specify the AD server and the AD domain (Figure 143).

Figure 143. Authentication > Add Realm

The screenshot shows the 'Add Realm' configuration page in the IronPort S370 interface. The page is titled 'Add Realm' and has a 'No Changes Pending' status. The configuration is for an 'NTLM Authentication Realm'. The 'Realm Name' is 'WSA Authn'. The 'Authentication Protocol and Scheme(s)' is 'NTLM (NTLMSSP or Basic Authentication)'. Under 'NTLM Authentication', the 'Active Directory Server' is '10.4.200.10' and the 'Active Directory Domain' is 'CISCO.LOCAL'. The 'Computer Account' is 'Computers'. A 'Join Domain' button is present. At the bottom, there is a 'Test Current Settings' section with a 'Start Test' button.

**Step 3:** Select the **Join Domain** button. When this is configured, AD Domain Administrator credentials (or an administrator to enter them) will be required to create domain accounts for computers (Figure 144).

Figure 144. AD Administrative Domain Logon

The screenshot shows the 'Add Realm' page with a 'Computer Account Credentials' dialog box open. The dialog prompts for 'Username' (administrator) and 'Password' (masked). A 'Create Account' button is visible.

**Step 4:** Once login credentials have been entered, click **Start Test** on the same page to test the NTLM connection to the AD domain.

If successful (Figure 145), Submit and Commit changes.

Figure 145. AD Test

The screenshot shows the 'Start Test' dialog box with the following text: 'Success: AD Server time and WSA time difference within tolerance limit', 'Attempting to fetch group information...', 'Success: Able to query for Group Information from Active Directory server '10.4.200.10'.', and 'Test completed successfully.'

The next step in setting up Authentication is to configure identity groups. Identities are based on the identity of the client or the transaction itself.

**Step 5:** Select **Web Security Manager > Identities**.

**Step 6:** Click **Add Identity**.

Two different sample identities will be created: "Subnets not to Authen" and "User Agents not to Authen."



**Step 7:** If the need arises to build an identity around subnets, insert the client IP address or range or subnet that you do not want to have to authenticate to access the Internet. Understand that performing this action defeats the purpose of running authentication for that IP address and that log information from the WSA will never have authentication data from employees using that IP address. Even so, taking this action might be required in certain cases and is given here as an example of how to change the operational policy of the WSA (Figure 146).

Figure 146. Example Identity: “Subnets not to Authen”

IronPort S370 Web Security Manager interface showing the configuration for a new identity named "Subnets not to Authen". The identity is enabled and its membership is defined by the subnet 10.4.200.1-254. The configuration includes options for enabling the identity, setting a name and description, and defining membership criteria by subnet, protocol, or authentication. The advanced section shows that no proxy ports, URL categories, or user agents are currently selected for this identity.

**Step 8:** The other Identity we will build is one for User Agents. Select the **Advanced** tab for User Agents and select **Microsoft Windows Update** and **Adobe Acrobat Updater** agent types. Selecting these agents means that when connections over HTTP with those User Agents in the HTTP Header are seen, no authentication will be requested. Custom User Agents can be defined for any application that uses HTTP and is failing authentication. If that is not possible, then a specific custom URL category can be built and then used in the Advanced tab for URL Categories (Figure 147).

Figure 147. Example Identity: “User Agents not to Authen”

IronPort S370 Web Security Manager interface showing the configuration for a new identity named "User Agents not to Authen". The identity is configured using the "Advanced Membership Definition: User Agents" tab. Under "Common User Agents", "Microsoft Windows Update" and "Adobe Acrobat Updater" are selected. The "Match User Agents" section is set to "Match the selected user agent definitions".

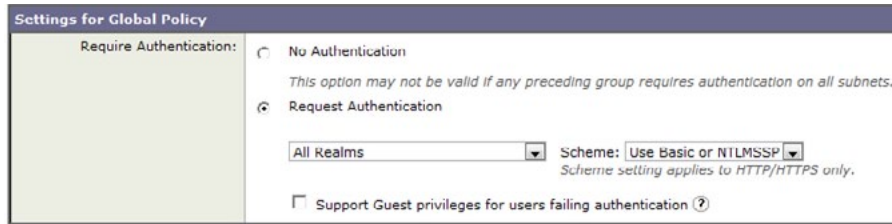
Now that two Identities have been built for “User Agents not to Authenticate” and “Subnets not to Authenticate”, there is one more step to complete the Authentication section.

**Step 9:** Select the link at the bottom of the Identities section labeled **Global Identity Policy**.

This is the identity group for anybody who does not meet one of the preceding two groups we just built. Since those groups were built for the purpose of not authenticating, change the global identity to authenticate everybody else.

**Step 10:** Change the group to Request Authentication for All Realms and to use **Basic** or **NTLMSSP** scheme (Figure 148).

Figure 148. Global Policy Settings



**Step 11:** Submit and Commit changes.

It is now possible to test the deployment to ensure that the system is enforcing policy as expected, that all applications and processes work as before, and that the data that the system logging meets all your needs or requirements.

## Internet Edge 10K Deployment

A single Cisco WSA S370 appliance was deployed in the Internet Edge 5K design. For those who need either the performance or the resilience offered by the Internet Edge 10K design, a simple upgrade solution is possible by adding an additional WSA S370 appliance. When deployed as above in the High Availability section, the two appliances will load share the outgoing connections. If one device fails, the load will be moved to the other WSA. It is possible that network performance could be degraded if one device is handling the load that was designed for two, but Internet web access will remain available and protected.

## Final Steps

### Monitoring

To monitor the health of the WSA and the actions being taken by the WSA on traffic it is examining, there are a variety of reports available under Monitor. These reports allow an administrator to track statistics for client web activity, malware types, web reputation filters, system status, and more.

Because the appliance itself only stores data for a limited amount of time, you need to install separate software from Sawmill to allow for long-term storage and reporting of events from the WSA.

Consult with your Cisco Account Team or your trusted Partner for more information on Sawmill and long-term reporting.

## Troubleshooting

To determine why the WSA took the action it did on a web connection to a specific site from a specific user, an administrator can run the Trace tool under **System Administration > Policy Trace**.

By filling out the tool, you can test a specific URL to find out what the expected response from the WSA would be if the URL were processed by the WSA. This information is especially useful if some of the more advanced features are used.

## Summary

You have now installed the Cisco Web Security Appliance. A basic configuration has been applied and the device can be inserted into the network and receive redirects from the ASA firewall. A default policy has been built that allows an agency to set up access controls for HTTP and HTTPS. A policy has been built to configure HTTPS decryption. And authentication has been set up to allow the WSA to authenticate users and tie username with the access controls in the logs.

A more detailed discussion about specific implementation of policy should be initiated with a trusted partner or Cisco account representative.

## Additional Information

User documentation can be found here:

<http://www.ironport.com/support/login.html>

Work with a Cisco IronPort Channel partner to obtain a login.

# Internet Edge Server Load Balancing

## Agency Overview

An agency's presence on the Internet plays a key role in the success of an agency. At a minimum web presence, a site that presents basic information about the agency is a requirement. It is important that this website has a high level of availability as the internet is a 24 x 7 operation and partners or customers could view the site at anytime. Downtime, even for a simple informational site means missed opportunities.

## Technology Overview

The Internet boom ushered in the era of the server load balancers (SLBs). The primary function of an SLB is to spread the load from clients across banks of servers to improve their response time and availability. Additional functionality provided by an SLB includes application proxies and complete Layer 4 through 7 application switching.

The Application Control Engine (ACE) is the latest SLB offering from Cisco. From its mainstream role in providing Layer 4 through 7 switching, ACE also provides an array of acceleration and server offload benefits, including TCP processing offload, Secure Socket Layer (SSL) offload, compression, and various other acceleration technologies. In the Internet Edge, the Cisco ACE sits in front of the web and application servers and provides a range of services to maximize server and application availability, security, and application acceleration. As a result, Cisco ACE can give an agency more control over application and server infrastructure, which enables it to manage and secure application services more easily and improves performance and availability.

As the next-generation Application Delivery Controller, Cisco ACE provides four key benefits:

- **Scalability.** ACE scales the performance of a server-based application, such as a web server, by distributing its client requests across multiple servers, known as a server farm. As traffic increases, additional servers can be added to the farm.

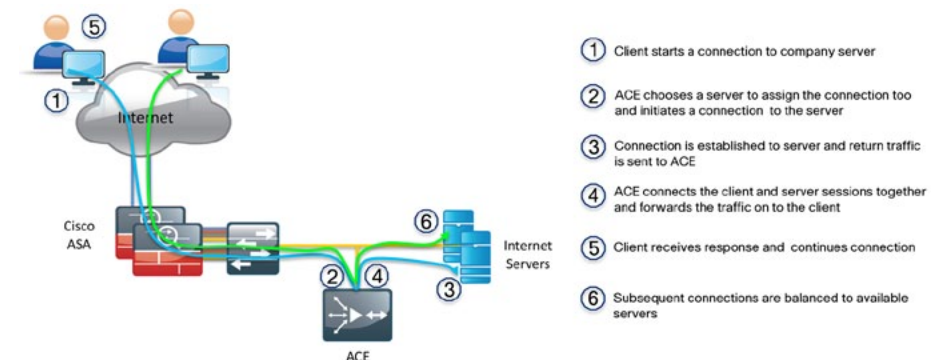
- **High Availability.** ACE provides high availability by automatically detecting the failure of a server and redirecting client traffic to remaining servers within seconds, thus providing users with continuous service.
- **Application Acceleration.** ACE improves application performance and reduces response time by minimizing latency and data transfers for any HTTP-based application, for any internal or external end user.
- **Server Offload.** ACE offloads TCP and SSL processing, which allows servers to serve more users and handle more requests without increasing the number of servers.

ACE hardware is always deployed in pairs for high availability: one primary and one secondary. If the primary ACE fails, the secondary ACE takes over. This failover can take place without disrupting the client-to-server connections.

Cisco ACE uses both active and passive techniques to monitor server health. By periodically probing servers, the ACE will rapidly detect server failures and quickly reroute connections to available servers. A variety of health-checking features are supported, including the ability to verify web servers, SSL servers, application servers, databases, FTP servers, streaming media servers, and a host of others.

Physically, the ACE appliance can be deployed in several ways. "One-armed" mode is the simplest deployment method. In this mode, the ACE resides on the same VLAN as the real servers. It is not directly in the path of traffic flow and only receives traffic that is specifically intended for it. Traffic is directed to the ACE and is controlled by the design of VLANs, virtual server addresses, and server default gateway selection (Figure 149).

Figure 149. ACE



## Configurations Details

In this configuration example, we first configure the ACE appliance with the basic network settings so it is accessible over the network. The second part of the configuration covers how to configure a policy for directing traffic to the web servers. The first part of the configuration is typically performed at the CLI when booting ACE for the first time, but both parts can be configured via the ACE GUI. Because the example load balancing configuration is simple, the setup in the deployment guide is shown using CLI commands.

### Procedure 1 Initial Setup

Procedure Steps:

1. Set system password
2. Configure basic access policy
3. Interface Setup
4. Setup high availability
5. Interface IP Configuration

#### Step 1: Set system password

When you set up the ACE for the first time, you must change the default password for the admin account.

```
switch login: admin
Password: admin
Admin user is allowed to log in only from console until the
default password is changed.
www user is allowed to log in only after the default password
is changed.
Enter the new password for user "admin": [admin password]
Confirm the new password for user "admin": [admin password]
admin user password successfully changed.
Enter the new password for user "www": [www password]
Confirm the new password for user "www": [www password]
www user password successfully changed.
Cisco Application Control Software (ACS)
TAC support: http://www.cisco.com/tac
Copyright © 1985-2009 by Cisco Systems, Inc. All rights
reserved.
The copyrights to certain works contained herein are owned
by other third parties and are used and distributed under
license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at http://www.gnu.
org/licenses/gpl.html.
ACE>
```

This script will perform the configuration necessary for a user to manage the ACE Appliance using the ACE Device Manager. The management port is a designated Ethernet port that has access to the same network as your management tools including the ACE Device Manager. You will be prompted for the Port Number, IP Address, Netmask, and Default Route (optional). Enter 'ctrl-c' at any time to quit the script  
ACE>Would you like to enter the basic configuration dialog (yes/no) [y]: n  
switch/Admin#

#### Step 2: Configure basic access policy

Before proceeding with additional configuration, you must set up basic network security policies to allow for management access into the ACE.

```
access-list ALL line 8 extended permit ip any any
class-map match-all http-vip
2 match virtual-address [Server Virtual IP] tcp eq www
class-map type management match-any remote_access
2 match protocol xml-https any
3 match protocol icmp any
4 match protocol telnet any
5 match protocol ssh any
6 match protocol http any
7 match protocol https any
8 match protocol snmp any
policy-map type management first-match remote_mgmt_allow_
policy
class remote_access
permit
```

#### Step 3: Interface Setup

Ethernet VLAN trunks to the network switching resources connect the ACE appliances. Two Gigabit Ethernet ports on each ACE need to be configured to trunk to the core switch:

```
interface gigabitEthernet 1/1
channel-group 1
no shutdown
interface gigabitEthernet 1/2
channel-group 1
no shutdown
interface gigabitEthernet 1/3
switchport trunk allowed vlan 12
no shutdown
interface port-channel 1
switchport trunk allowed vlan 1121
no shutdown
```

The switch ports that connect to the security appliances must be configured so that they are members of the same secure VLANs and forward secure traffic to switches that offer connectivity to servers and other appliances in the server room.

The ACE appliances are configured for Active-Standby High Availability. When ACE appliances are configured in Active-Standby mode, the Standby appliance does not handle traffic, so the primary device must be sized to provide enough throughput to address connectivity requirements between the core and the server room.

A fault-tolerant (FT) VLAN is a dedicated VLAN used by a redundant ACE pair to communicate heartbeat and state information. All redundancy-related traffic is sent over this FT VLAN, including heartbeats, configuration sync packets, and state replication packets.

#### Step 4: Set up high availability

```
ft interface vlan 12
ip address [Failover Primary IP] 255.255.255.0
peer ip address [Failover Secondary IP] 255.255.255.0
no shutdown
ft peer 1
heartbeat interval 300
heartbeat count 10
ft-interface vlan 12
ft group 1
peer 1
priority 120
peer priority 110
associate-context Admin
inservice
```

#### Step 5: Interface IP Configuration

For the ACE to begin passing traffic, we need to create a VLAN interface and assign an IP address to it. Because we are employing one-armed mode, we need to create a NAT pool as well.

```
interface vlan 1121
ip address [Interface IP] 255.255.255.0
peer ip address [Peer IP] 255.255.255.0
access-group input ALL
nat-pool 1 [NAT IP] [NAT IP] netmask 255.255.255.0 pat
service-policy input remote_mgmt_allow_policy
no shutdown
ip route 0.0.0.0 0.0.0.0 [Default Gateway IP]
```

The following is the configuration generated and used in the lab from procedure one.

```
peer hostname ace-4710-2
hostname ace-4710-1
interface gigabitEthernet 1/1
channel-group 1
no shutdown
interface gigabitEthernet 1/2
channel-group 1
no shutdown
interface gigabitEthernet 1/3
switchport trunk allowed vlan 12
no shutdown
interface port-channel 1
switchport trunk allowed vlan 1121
no shutdown
```

```
access-list ALL line 8 extended permit ip any any
class-map match-all http-vip
2 match virtual-address 10.4.245.100 tcp eq www
class-map type management match-any remote_access
2 match protocol xml-https any
3 match protocol icmp any
4 match protocol telnet any
5 match protocol ssh any
6 match protocol http any
7 match protocol https any
8 match protocol snmp any
```

```
policy-map type management first-match remote_mgmt_allow_
policy
class remote_access
permit
```

```
interface vlan 1121
ip address 10.4.245.22 255.255.255.0
peer ip address 10.4.245.21 255.255.255.0
access-group input ALL
nat-pool 1 10.4.245.99 10.4.245.99 netmask 255.255.255.0 pat
service-policy input remote_mgmt_allow_policy
service-policy input int1121
no shutdown
```

```
ft interface vlan 12
ip address 10.10.12.11 255.255.255.0
peer ip address 10.10.12.12 255.255.255.0
no shutdown
```



```

ft peer 1
 heartbeat interval 300
 heartbeat count 10
 ft-interface vlan 12
ft group 1
 peer 1
 peer priority 110
 associate-context Admin
 inservice

ip route 0.0.0.0 0.0.0.0 10.4.245.1

```

At this point, the ACE should be reachable on the network. Now we can begin configuring a load-balancing policy.

## Procedure 2 Configure Load Balancing

Procedure Steps:

1. Define Servers
2. Setup server health monitoring
3. Define Server Farm
4. Setup load balancing policy

### Step 1: Define Servers

Start by defining the application servers that require load balancing:

```

rserver host webserver1
ip address [Web Server 1 IP]
inservice
rserver host webserver2
ip address [Web Server 2 IP]
inservice

```

### Step 2: Setup server health monitoring

This creates a simple HTTP probe to test the health of the web servers:

```

probe http http-probe
port 80
interval 15
passdetect interval 60
request method head
expect status 200 200
open 1

```

### Step 3: Define Server Farm

Place the web servers and the probe into a server farm:

```

serverfarm host webfarm
probe http-probe
rserver webserver1 80
inservice
rserver webserver2 80
inservice

```

### Step 4: Setup load balancing policy

Configure the load-balancing policy and assign it to the VLAN interface:

```

class-map match-all http-vip
2 match virtual-address [Server Virtual IP] tcp eq www
policy-map type loadbalance first-match http-vip-l7slb
class class-default
serverfarm webfarm
policy-map multi-match int1121
 class http-vip
 loadbalance vip inservice
 loadbalance policy http-vip-l7slb
 loadbalance vip icmp-reply active
 nat dynamic 1 vlan 1121
interface vlan 1121
service-policy input int1121

```

The following is the configuration generated and used in the lab from procedure two.

```

rserver host webserver1
ip address 10.4.245.112
inservice
rserver host webserver2
ip address 10.4.245.113
inservice
probe http http-probe
port 80
interval 15
passdetect interval 60
request method head
expect status 200 200
open 1
serverfarm host webfarm
probe http-probe
rserver webserver1 80
inservice

```

```
rserver webserver2 80
inservice
class-map match-all http-vip
 2 match virtual-address 10.4.245.100 tcp eq www
 policy-map type loadbalance first-match http-vip-l7slb
 class class-default
 serverfarm webfarm
policy-map multi-match int1121
 class http-vip
loadbalance vip inservice
loadbalance policy http-vip-l7slb
loadbalance vip icmp-reply active
nat dynamic 1 vlan 1121
interface vlan 1121
service-policy input int1121
```

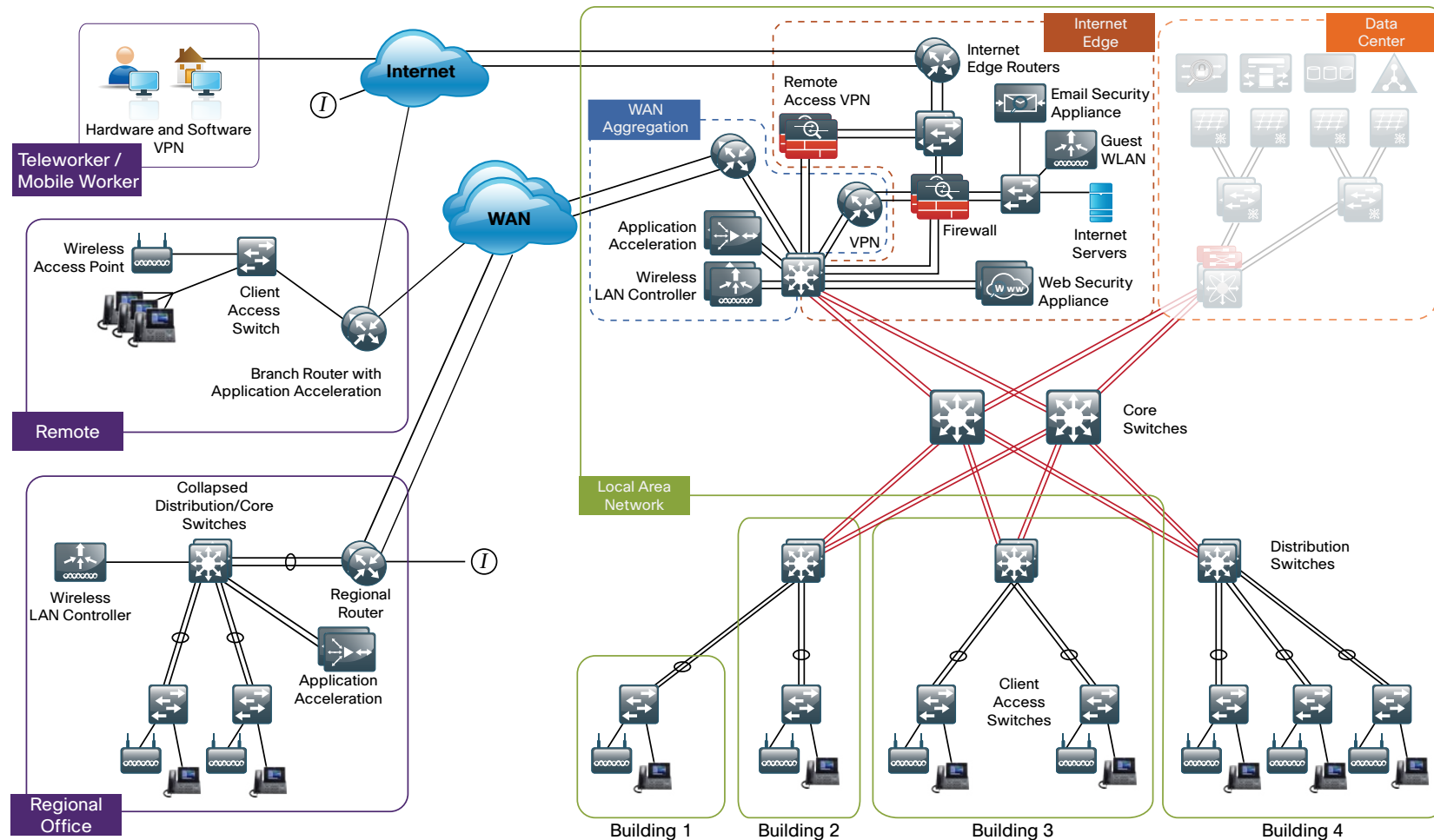
At this point, the application should be accessible via the VIP we created (10.4.245.100) and the requests should be distributed between the two web servers.

## Summary

IT organizations face significant challenges associated with the delivery of applications at the Internet Edge to a global group of partners, clients, and the public. Application-delivery technologies help agencies improve availability, performance, and security of all applications. The Cisco Application Control Engine provides core-server load-balancing services, advanced application acceleration, and security services to maximize application availability, performance, and security. It is coupled with unique virtualization capabilities, application-specific intelligence, and granular role-based administration to consolidate application infrastructure, reduce deployment costs, and minimize operational burdens.

## Notes

# Summary



This deployment guide is a reference design for Cisco customers and partners. It covers the Internet Edge component of Borderless Networks for Large Agencies and is meant to be used in conjunction with the *Cisco SBA for Large Agencies—Borderless Networks LAN Deployment Guide* and *WAN Deployment Guide*, which can be found at [www.cisco.com/go/sba](http://www.cisco.com/go/sba). If your network is beyond the scale of this design, please refer to the Cisco Validated Designs (CVD) for larger deployment models. CVDs can be found on Cisco.com. The Cisco products used in this design were tested in a network lab at Cisco. The specific products are listed at the end of this document for your convenience. A separate document, the Internet Edge Configuration Guide, contains the specific configuration files from the products used in the Cisco lab testing and can be found on Cisco.com.

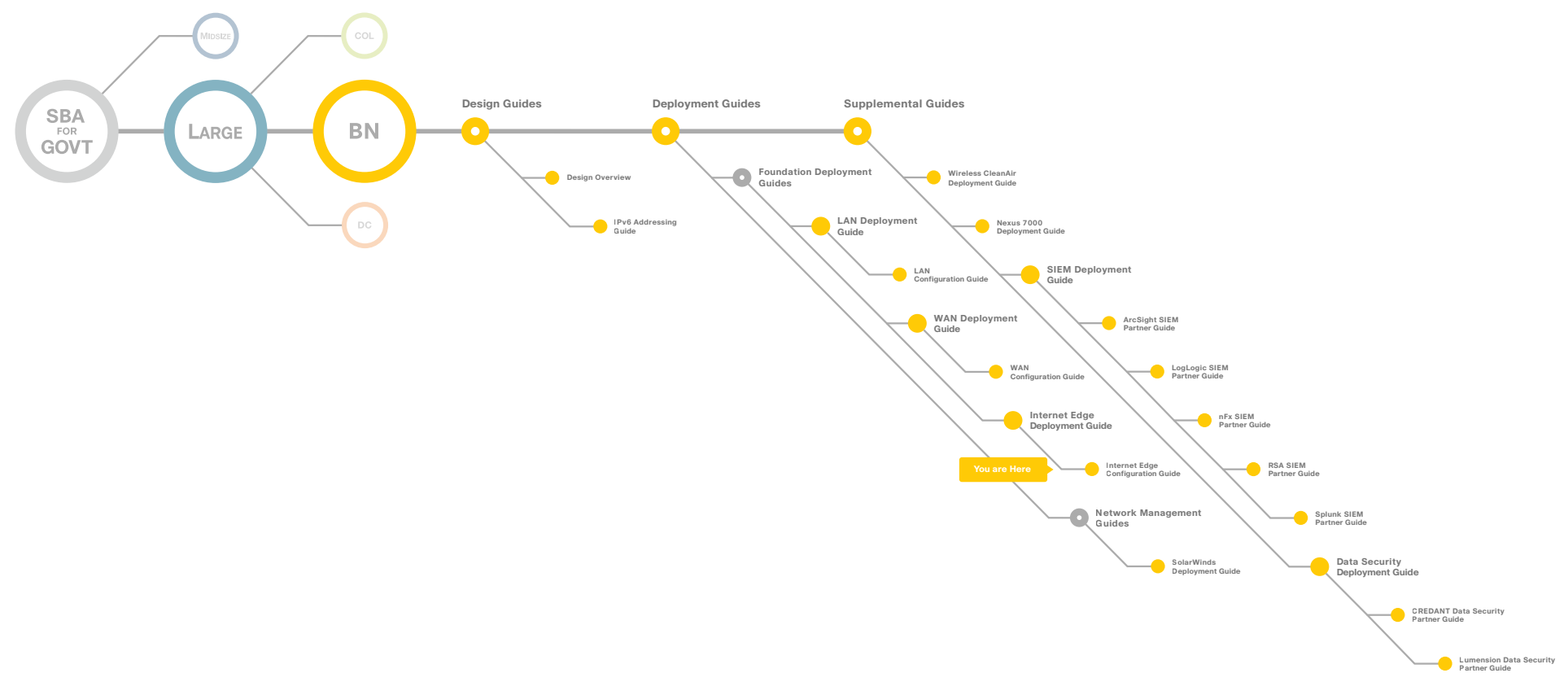
# Appendix A: Large Agencies Deployment Product List

| Functional Area                     | Product                                      | Part Numbers                                                                                         | Software Version |
|-------------------------------------|----------------------------------------------|------------------------------------------------------------------------------------------------------|------------------|
| <b>Internet Edge 5K</b>             |                                              |                                                                                                      |                  |
| Firewall                            | ASA 5510 or<br>ASA 5520 or<br>ASA 5540       | ASA5510-AIP10-SP-K9<br>ASA5520-AIP20-K9<br>ASA5540-AIP40-K9                                          | 8.2.2            |
| IPS                                 | SSM-AIP-10 or<br>SSM-AIP-20 or<br>SSM-AIP-40 | *part of the firewall bundle                                                                         | 7.0.2E4          |
| Software license for main<br>ASA FW | 250 or 500 SSL Session Software license      | ASA5500-SSL-250<br>ASA5500-SSL-500                                                                   | *as Firewall     |
| Email Security                      | C370                                         | C370-BUN-R-NA<br>*Please consult Trusted Partner or Ironport Sales Team for<br>pricing and licensing | Async OS 7.0     |
| Web Security                        | S370                                         | S370-BUN-R-NA<br>*Please consult Trusted Partner or Ironport Sales Team for<br>pricing and licensing | Async OS 6.3     |
| Server Load Balancing               | ACE 4710                                     | ACE-4710-0.5F-K9                                                                                     | A3(2.2)          |
| Outside Switch                      | 2x Catalyst 3750                             | WS-C3750G-24TS-S1U                                                                                   | 12.2(53)SE1      |
| DMZ Switch                          | 2x Catalyst 3750                             | WS-C3750G-24TS-S1U                                                                                   | 12.2(53)SE1      |
| <b>Internet Edge 10K</b>            |                                              |                                                                                                      |                  |

| Functional Area       | Product                                                            | Part Numbers                                                                                      | Software Version |
|-----------------------|--------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|------------------|
| Firewall              | 2x ASA 5520 or<br>2x ASA 5540                                      | ASA5520-AIP20-K9<br>ASA5540-AIP40-K9                                                              | 8.2.2            |
| IPS                   | 2x SSM-AIP-20 or<br>2x SSM-AIP-40                                  | *part of bundle above                                                                             | 7.0.2E4          |
| VPN                   | 2x ASA 5520 and 500 SSL seats or<br>2x ASA 5540 and 1000 SSL seats | ASA5520-SSL500-K9<br>ASA5540-SSL1000-K9                                                           | 8.2.2            |
| Email Security        | 2x C370                                                            | C370-BUN-R-NA<br>*Please consult Trusted Partner or Ironport Sales Team for pricing and licensing | Async OS 7.0     |
| Web Security          | 2x S370                                                            | S370-BUN-R-NA<br>*Please consult Trusted Partner or Ironport Sales Team for pricing and licensing | Async OS 6.3     |
| Server Load Balancing | ACE 4710                                                           | ACE-4710-1F-K9                                                                                    | A3(2.2)          |
| Outside Switch        | 2x Catalyst 3750                                                   | WS-C3750G-24TS-S1U                                                                                | 12.2(53)SE1      |
| DMZ Switch            | 2x Catalyst 3750                                                   | WS-C3750G-24TS-S1U                                                                                | 12.2(53)SE1      |



# Appendix B: SBA for Large Agencies Document System





SMART BUSINESS ARCHITECTURE



**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV  
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

C07-640806-00 12/10