Newer Cisco SBA Guides Available

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

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

Internet Edge Deployment Guide

SMART BUSINESS ARCHITECTURE

February 2012 Series

Preface

Who Should Read This Guide

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

Release Series

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.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

month year Series

For example, the series of guides that we released in August 2011 are the "August 2011 Series".

You can find the most recent series of SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

How to Read Commands

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

Commands shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100
100 100 100
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

Comments and Questions

If you would like to comment on a guide or ask questions, please use the forum at the bottom of one of the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

An RSS feed is available if you would like to be notified when new comments are posted.

Table of Contents

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 NONINFRINGEMENT 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.

What's In This SBA Guide

About SBA

Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.

For more information, see the *How to Get Started with Cisco SBA* document:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Smart_Business_Architecture/SBA_Getting_Started.pdf

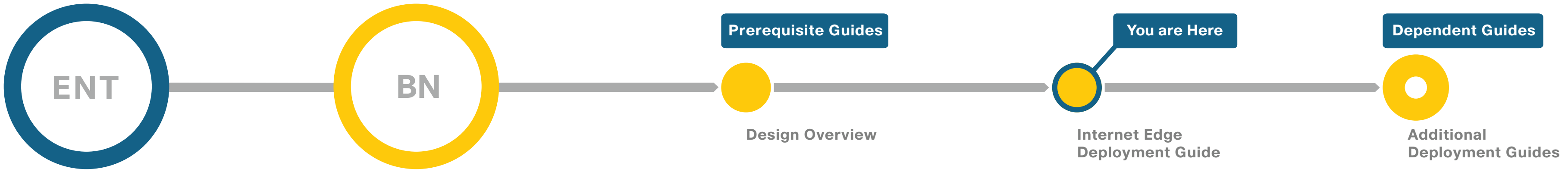
About This Guide

This *foundation deployment guide* is organized in sections, which each include the following parts:

- Business Overview—The challenge your organization faces. Business decision makers can use this part to understand the relevance of the solution to their organizations' operations.
- Technology Overview—How Cisco solves the challenge. Technical decision makers can use this part to understand how the solution works.
- Deployment Details—Step-by-step instructions for implementing the solution. Systems engineers can use this part to get the solution up and running quickly and reliably.

To learn what changed in this guide between the previous series and the current series, see Appendix B: Changes.

This guide presumes that you have read the prerequisite foundation design overview, as shown on the Route to Success below.



Route to Success

To ensure your success when implementing the designs in this guide, you should read any guides that this guide depends upon—shown to the left of this guide on the route above. Any guides that depend upon this guide are shown to the right of this guide.

For customer access to all SBA guides: http://www.cisco.com/go/sba
For partner access: http://www.cisco.com/go/sbachannel

Introduction

Cisco SBA for Enterprise Organizations—Borderless Networks is a solid network foundation designed to provide networks with 2,000 to 10,000 connected users the flexibility to support new users or network services without re-engineering the network. 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 foundation architecture is described in a single *Design Guide*, as well as several deployment and configuration guides for each of the three parts of the foundation: LAN, WAN, and Internet Edge.

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

Related Reading

The *Design Guide* orients you to the overall Cisco SBA design and explains the requirements that were considered when selecting specific products.

The *Local Area Network Deployment Guide* describes 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.

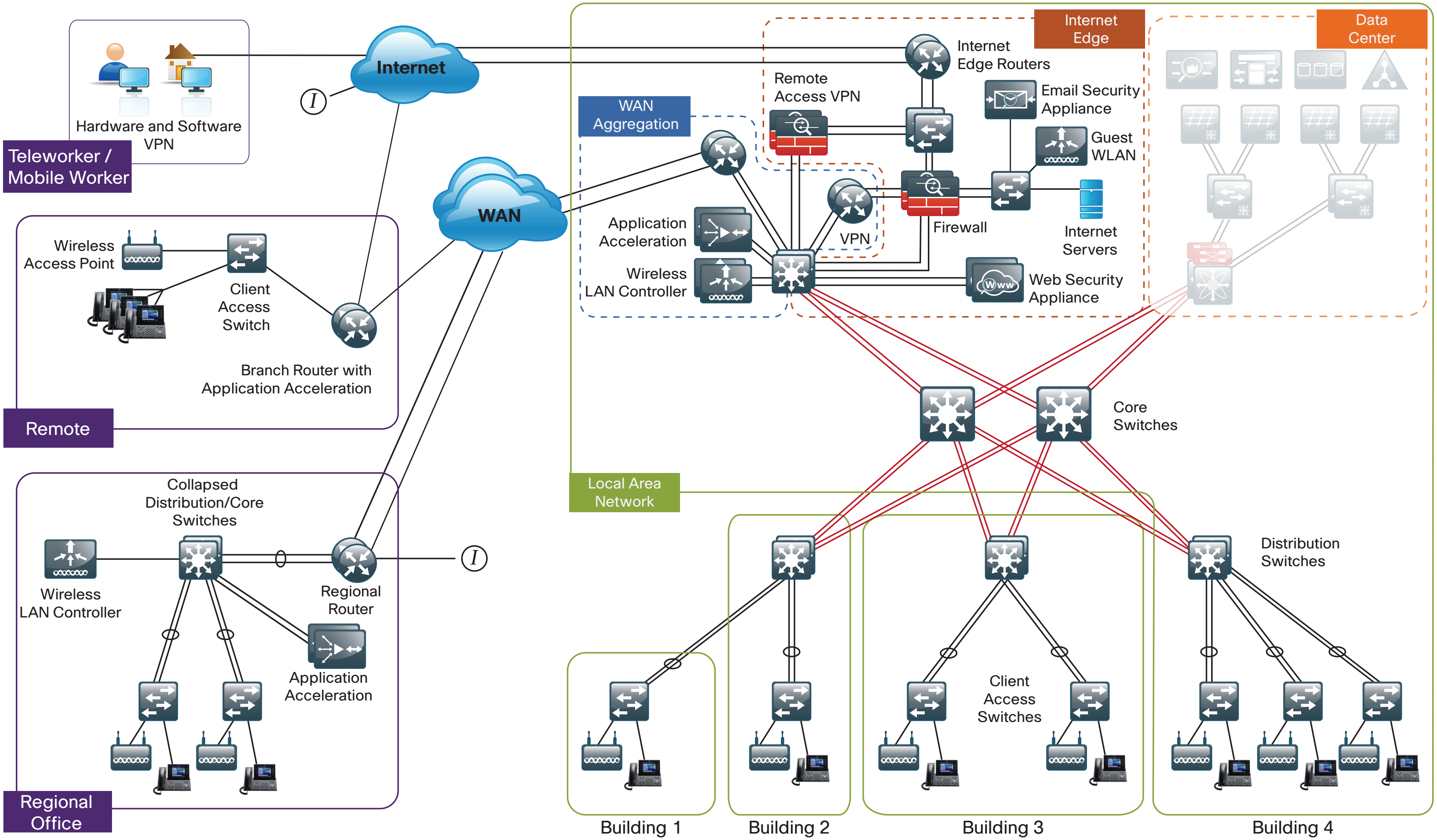
To help focus on specific elements of the architecture, there are three WAN deployment guides:

- *WAN Deployment Guide* provides flexible guidance and configuration for Multiprotocol Label Switching (MPLS) transport as well as broadband or Internet transport in a backup role.
- *Layer 2 WAN Deployment Guide* provides guidance and configuration for a VPLS or Metro Ethernet transport as well as a broadband or Internet transport in a backup role.
- *VPN Remote Site Deployment Guide* provides guidance and configuration for broadband or Internet transport in a both a primary or backup role

Design Goals

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

Figure 1 - Borderless Networks for Enterprise Organizations Overview



Ease of Deployment, Flexibility, and Scalability

Organizations with 2000 to 10,000 users are often spread out among different geographical locations, making flexibility and scalability a critical requirement of the network. This design uses several methods to create and maintain a scalable network:

- By keeping a small number of standard designs for common portions of the network, support staff is able to design services for, implement, and support the network more effectively.
- Our modular design approach enhances scalability. Beginning with a set of standard, global building blocks, we can assemble a scalable network to meet requirements.
- Many of the plug-in modules look identical for several service areas; this common look provides consistency and scalability in that the same support methods can be used to maintain multiple areas of 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 appropriate redundancy to guard against failure in the network. The redundancy in our architecture is carefully balanced with the complexity inherent in redundant systems.

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.

Network security is also a 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.

Ease of Management

While this guide focuses on the deployment of the network foundation, the design takes next phase management and operation into consideration. The configurations in the deployment guides are designed to allow the devices to be managed via normal device management connections, such as SSH and HTTPS, as well as 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 organization 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.
- The wireless network is 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 ready to provide soft phones via VPN, as well as traditional hard or desk phones.

Internet Edge Business Overview

Organizations must meet the following requirements and address these issues:

- Organizations need to provide users access to Internet services (email and web).
- Users need access to services inside the organization from remote locations.
- Organizations need to provide controlled access to data and/or services for the public, partners, and customers.
- Organizations need to improve employee productivity by restricting Internet access to non-work-related locations.

Organizations need to manage security risk associated with Internet connectivity. The Internet Edge provides connectivity for traffic traversing between the organization and the Internet. This includes traffic to and from the organization, the Internet, and demilitarized zones (DMZ). An organization's Internet Edge deployment needs to enforce the organization's 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.

The Internet Edge also provides users remote access to the services and data they require to perform their role, from any location. In borderless networks, a user could be an employee, a contractor, a partner, or a customer. Each user has different needs for access, data, and services.

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 a file that contains malicious code. The result of not protecting the organization against this activity includes loss of intellectual property, data theft, or even potential legal liability.

Architecture Overview

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

The Internet Edge design includes the following modules:

- **Firewall**—Controls access into and out of the different segments of the Internet Edge and provides a suite of other services, such as Network Address Translation (NAT)
- **Intrusion Prevention**—Inspects traffic traversing the Internet Edge, looking for malicious behaviors
- **Remote Access VPN**—Provides secure, consistent access to resources, regardless of where the user is when connecting
- **Email Security**—Provides SPAM and malware filtering service to manage the risk associated with email
- **Web Security**—Provides acceptable-use control and monitoring while managing the increasing risk associated with clients browsing the Internet
- **Internet Edge Server Load Balancing**—Balances web services to the public and private network

The requirements for each organization differ based on many factors. The number of users in an organization is a good starting point, so SBA for Enterprise Organizations provides two designs based on user count: Internet Edge 5K and Internet Edge 10K.

Figure 2 - Internet Edge in the Borderless Networks for Enterprise design

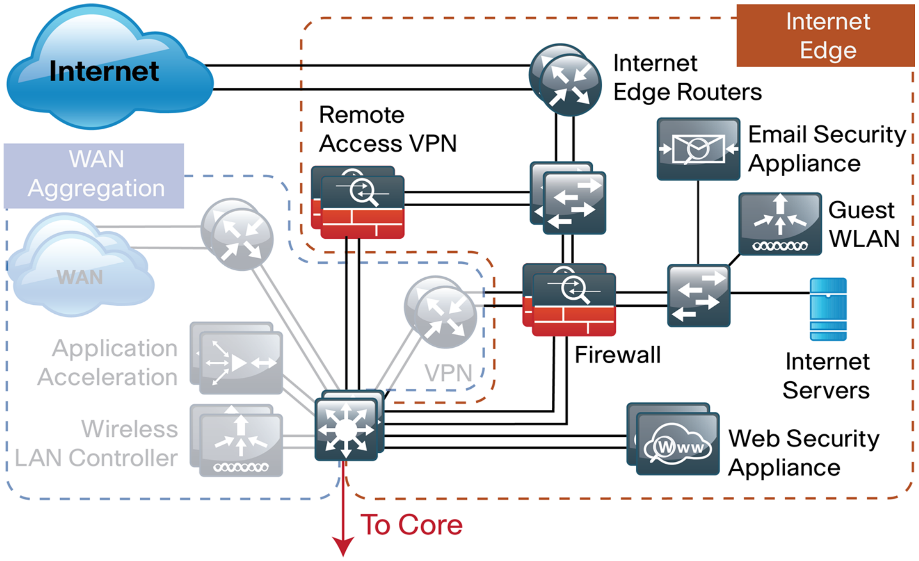


Figure 3 - Internet Edge 5K design

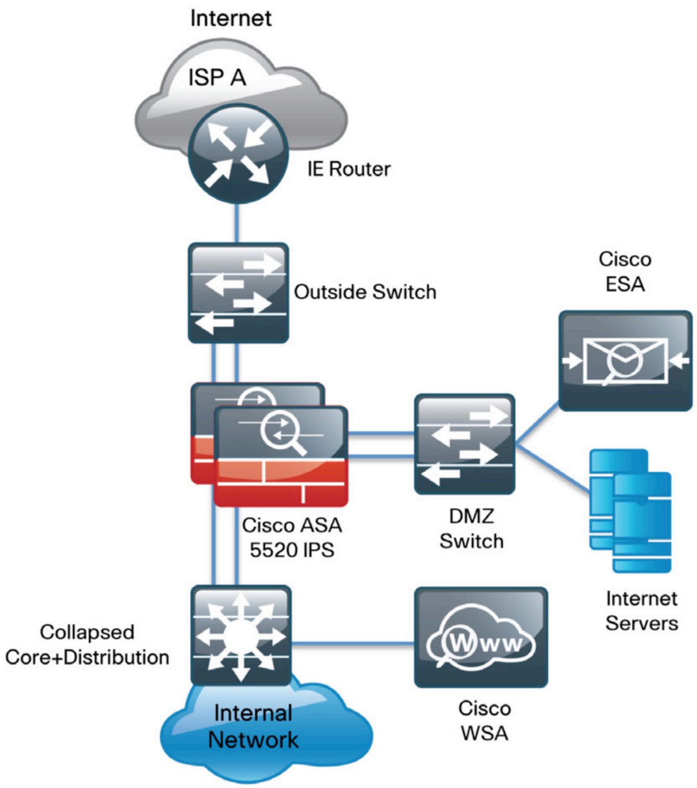
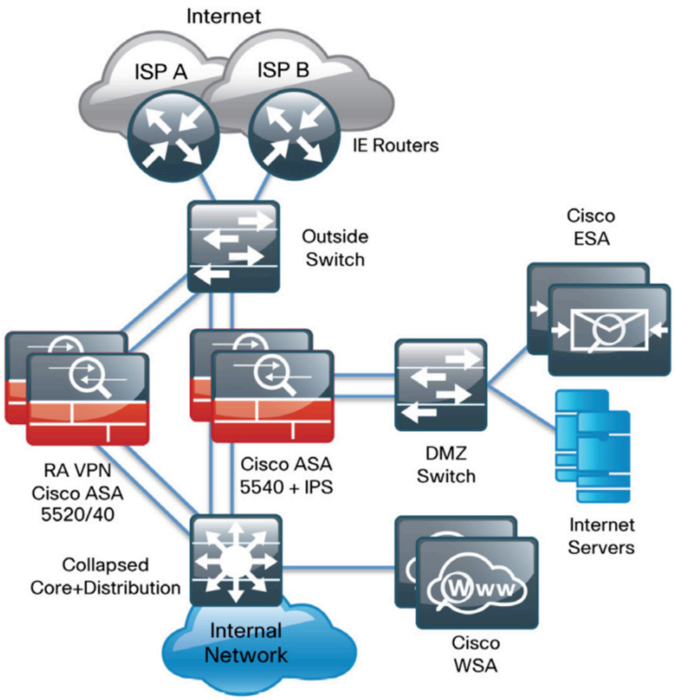


Figure 4 - Internet Edge 10K design



The primary differences between the two designs are scale, performance, and resilience. The Internet Edge 5K design is typical for an organization with up to 5,000 connected users, and the Internet Edge 10K design is for organizations with 5,000 to 10,000 connected users. These designs differ in the number of users that the devices can support and the number of ISPs the organization uses to connect to the Internet. To accommodate these requirements, each module of the Internet Edge Deployment Guide is independent of the others, so you can mix and match the different design components to best meet your business requirements. For example, an organization with fewer than 5,000 users might choose to use the Internet Edge 10K design for remote access if it has a highly mobile workforce and the remote-access requirements are higher than average.

Finally, the Internet Edge 5K, offers a single connection to one ISP; and the 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.

Internet Edge Connectivity

Business demand for Internet connectivity has increased steadily over the last few decades; for many organizations, 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 businesses to pursue their missions. An Internet connection that supports these services must be designed to enable the organization to accomplish its Internet-based business goals.

Three factors define the business requirements for an organization's Internet connection:

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

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

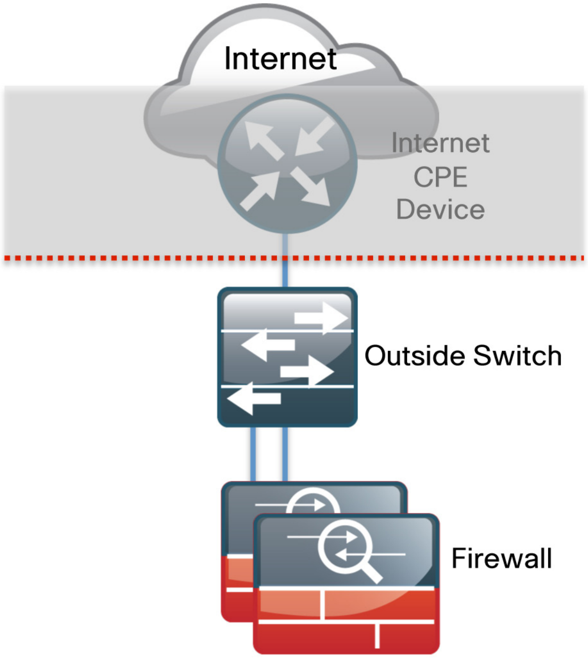
Internet connection speed, availability, and address space requirements are criteria that will shape an Internet connection design. The Internet connection must be able to accommodate an organization's requirements for data volume to the Internet, offer sufficient resiliency to meet service-level agreements, and provide sufficient IP address space to accommodate both Internet-facing and Internet-based services.

An organization'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 organization or one that does not rely heavily on web-based services to the Internet will have a different IP space requirement than a large organization 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.

Internet connectivity options vary widely by geographic region and service provider. An organization 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 5 - Internet connectivity demarcation for this design



Organizations 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
2,000 to 4,500	20–50 Mbps
3,000 to 7,000	35–75 Mbps
6,000 to 10,000	70–130 Mbps

If the business 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. The organization must assess the impact of configuration-change lead times and configuration flexibility.

The following table depicts recommendations for Internet access platform selection.

Table 2 - Internet access platform recommendations

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

Regardless of how access is delivered, design and configuration discussions for this guide begin at the Ethernet handoff on the outside switch in the Internet Edge.

High Availability Overview

The decision to use a single or dual Internet connection should be made on your organization's connection availability requirements. If a loss of Internet access will cause a business interruption that has a greater cost impact than the cost of a backup Internet connection, then the Internet Edge 10K design should be used. A backup Internet connection assures 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 the following:

- Resilient outbound Internet access and inbound email services.
- Additional inbound services that can be provisioned to recover in the event of a failure, although some services may experience longer outages.
- Inbound web service that does not have seamless failover protection and requires user interaction to point the Domain Name System (DNS) records at the alternate IP address on the secondary ISP. To achieve higher web-service availability, an organization can host its web service at a colocation facility or use a fully redundant Border Gateway Protocol (BGP) design that advertises the same IP address out to different ISPs. Organizations 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. BGP and other dynamic routing options offer various methods to influence Internet routing. For the majority of organizations with 2,000 to 10,000 connected users, a static default route is adequate to establish access to the Internet and has the least operational complexity.

Reader Tip

If an organization's routing requirements exceed what can be addressed by static routing, refer to the *Cisco Enterprise Internet Edge Design Guide,* which covers more complex Internet connectivity deployments:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/IE_DG.html

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. These configurations are sufficient for organizations of 2,000 to 10,000 connected users that are not hosting critical content or eCommerce in their DMZ. In the 10K design, Internet Control Message Protocol (ICMP) probes are sent to an Internet IP address from the Cisco Adaptive Security Appliance (Cisco ASA) firewalls. If the 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 email (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.

Reader Tip

The 10K design does not address multi-homed routing options, e.g., using BGP with multiple Internet connections to multiple ISPs. For more information on multi-homed Internet connectivity designs, refer to the *Cisco Enterprise Internet Edge Design Guide* in the Cisco Design Zone:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/IE_DG.html

Firewall

Business Overview

The Internet edge is the point where the organization'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 with an organization's network. Worm, virus, and botnet infiltrations pose substantial threats to network performance, availability, and data security. To add to these problems, an organizations' Internet connection can contribute to employee productivity loss and leakage of confidential data.

Internet-based attackers are a threat to an organization's network infrastructures and data resources. Most networks connected to the Internet are subject to a constant barrage of worms, viruses, and targeted attacks. Organizations must vigilantly protect 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.

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

Firewall security is an integral part of every Internet Edge deployment, as it protects information while meeting the need for secure reliable networks and enforces policy in order to maintain employee productivity. Where industry regulations apply, firewalls play a crucial role in an organization's ability to address regulatory compliance requirements. Regulatory requirements vary by country and industry; this document does not cover specific regulatory compliance requirements.

Technology Overview

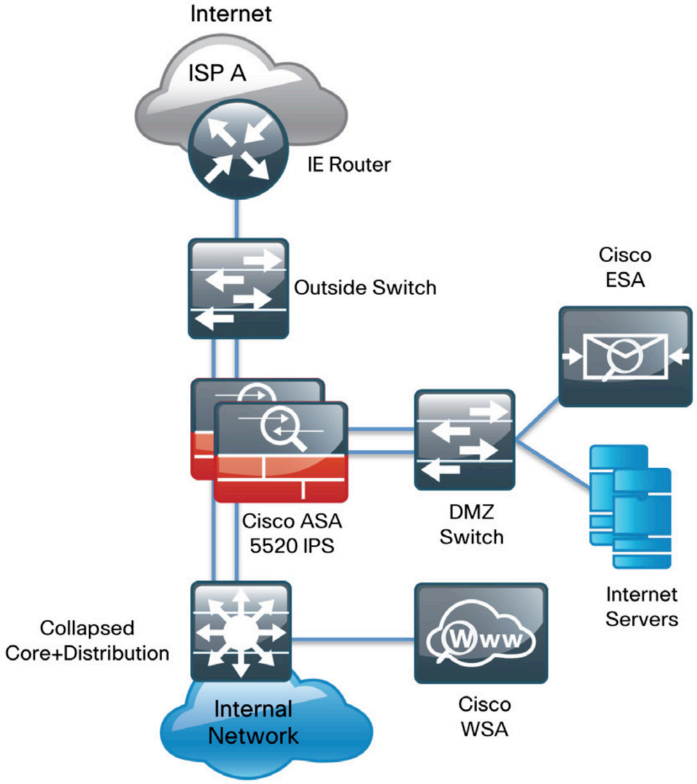
The Cisco ASA firewall family sits between the organization's internal network and the Internet and is a fundamental infrastructural component that minimizes the impact of network intrusions while maintaining worker productivity and data security.

This design uses Cisco ASA 5500s for Internet Edge firewall security. They are configured in an active/standby pair for High Availability in order 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 Network Address Translation (NAT) and firewall policy, and they host Intrusion Prevention System Security Services Modules (AIP-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.

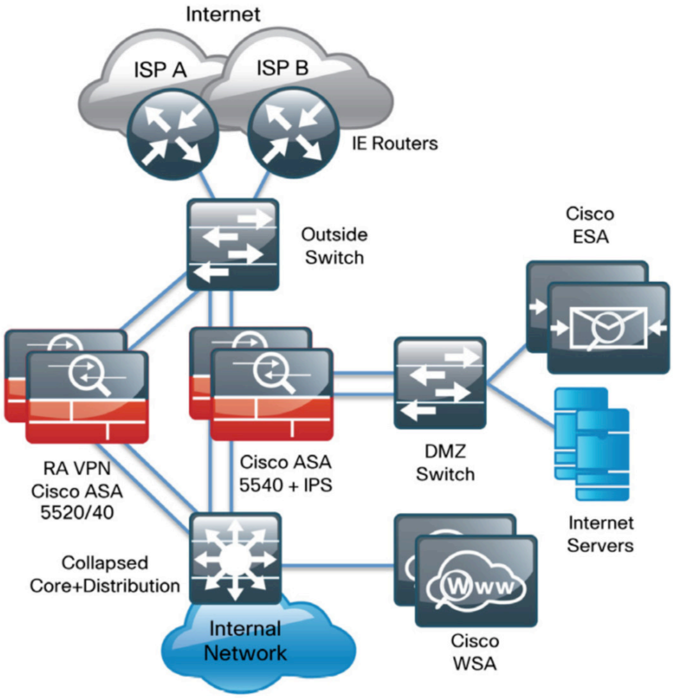
The Internet Edge 5K firewall design uses a single Internet connection and integrates the remote-access VPN function in the same Cisco ASA pair that provides the firewall functionality.

Figure 6 - Internet Edge 5K topology



The Internet Edge 10K firewall design uses dual Internet connections for resilient access to the Internet. A separate pair of appliances provides remote-access VPN, allowing additional scalability and operational flexibility.

Figure 7 - 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 is mentioned in that section.

The configurations are for any of the one-rack-unit Cisco 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 Cisco 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

Deployment Details

Process

Configuring the Firewall

1. Configure the LAN distribution switch
2. Apply Cisco ASA initial configuration
3. Configure internal routing
4. Configure user authentication
5. Configure time synchronization and logging
6. Configure device management protocols

The Cisco ASA can be configured from the command line or from the graphical user interface, Cisco Adaptive Security Device Manager (ASDM). Cisco ASDM is the primary method of configuration illustrated in this deployment guide. This process uses the command line to initially configure the appliance and then uses Cisco ASDM to manage the configuration.

Only the primary Cisco ASA in the High Availability (HA) pair needs to be configured. The Configuring Firewall High Availability process will set up HA and synchronize the configuration from the primary to the secondary device.

Procedure 1 Configure the LAN distribution switch

The LAN distribution switch is the path to the organization's internal network. A unique VLAN supports the Internet Edge devices, and the routing protocol peers with the appliances across this network.

Reader Tip

This procedure assumes that the distribution switch has already been configured following the guidance in the *Smart Business Architecture—Borderless Networks for Enterprise Organizations LAN Deployment Guide*. Only the procedures required to support the integration of the firewall into the deployment are included in this guide.

Step 1: Configure the Internet Edge VLAN and switched virtual interface (SVI).

```
vlan 300
 name InternetEdge
!
spanning-tree vlan 300 root primary
!
interface vlan 300
 description Internet Edge SVI
 ip address 10.4.24.1 255.255.255.224
```

Step 2: Configure the interfaces that are connected to the Internet Edge firewall.

```
interface GigabitEthernet1/0/24
 description IE-ASA5540a Gig0/0
!
interface GigabitEthernet2/0/24
 description IE-ASA5540b Gig0/0
!
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
 switchport access vlan 300
 switchport host
 macro apply EgressQoS
```

Step 3: Summarize the Internet Edge network range towards the core.

```
interface range TenGigabitEthernet1/1/1, 
TenGigabitEthernet2/1/1
 ip summary-address eigrp 100 10.4.24.0 255.255.248.0
```

Step 4: Configure the routing protocol to form neighbor relationships on the Internet Edge VLAN.

```
router eigrp 100
  no passive-interface Vlan300
```

Procedure 2 Apply Cisco ASA initial configuration

This procedure configures connectivity to the appliance from the internal network in order to enable management access.

Step 1: Configure the appliance host name.

```
hostname IE-ASA5540
```

Step 2: Configure the appliance interface that is connected to the internal LAN distribution switch.

```
interface GigabitEthernet0/0
 nameif inside
 ip address 10.4.24.30 255.255.255.224
 no shutdown
```

Step 3: Disable the dedicated management interface.

```
interface Management0/0
 shutdown
```

Procedure 3 Configure internal routing

A dynamic routing protocol is used to easily configure reachability between networks connected to the appliance and those that are internal to the organization.

Step 1: Enable Enhanced Interior Gateway Routing Protocol (EIGRP) on the appliance.

```
router eigrp 100
```

Step 2: Configure the appliance to advertise its statically defined routes and connected networks that are inside the Internet Edge network range.

```
 no auto-summary
 network 10.4.24.0 255.255.252.0
 redistribute static
```

Step 3: Configure EIGRP to peer with neighbors across the inside interface only.

```
 passive-interface default
 no passive-interface inside
```

Step 4: Configure a network object for the summary address of the internal network. The network object will be used later during security policy configuration.

```
object network internal-network
 subnet 10.4.0.0 255.254.0.0
 description The organization's internal network range
```

Procedure 4 Configure user authentication

Authentication, authorization and accounting (AAA) is enabled for access control. AAA controls all management access to the network infrastructure devices (SSH and HTTPS).

Reader Tip

The AAA server used in this architecture is the Cisco Secure Authentication Control System (ACS). Configuration of Cisco Secure ACS is discussed in the *Network Device Authentication and Authorization Deployment Guide.*

Management logins from infrastructure devices to the AAA server use TACACS+ as the primary protocol. A local AAA user database is also defined on each network infrastructure device in order to provide a fallback authentication source in case the centralized TACACS+ server is unavailable.

Step 1: Configure a local user for fallback authentication.

```
username admin password c1sco123 privilege 15
```

Step 2: Configure the TACACS+ server.

```
aaa-server AAA-SERVER protocol tacacs+
aaa-server AAA-SERVER (inside) host 10.4.48.15 SecretKey
```

Step 3: Configure the appliance's management authentication to use the TACACS+ server first and then the local user database if the TACACS+ server is unavailable.

```
aaa authentication enable console AAA-SERVER LOCAL
aaa authentication ssh console AAA-SERVER LOCAL
aaa authentication http console AAA-SERVER LOCAL
aaa authentication serial console AAA-SERVER LOCAL
```

Step 4: Configure the appliance to use AAAA to authorize management users.

```
aaa authorization exec authentication-server
```

Tech Tip

User authorization on the Cisco ASA firewall does not automatically present the user with the enable prompt if they have a privilege level of 15, unlike Cisco IOS devices.

Procedure 5 Configure time synchronization and logging

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

The Network Time Protocol (NTP) is designed to synchronize time across a network of devices. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the organization's network.

Network devices should be programmed to synchronize to a local NTP server in the network. The local NTP server typically references a more accurate clock feed from an outside source.

There is a range of detail that can be logged on the appliance. Informational-level logging provides the ideal balance between detail and log-message volume. Lower log levels produce fewer messages, but they do not produce 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.

Step 1: Configure the NTP server.

```
ntp server 10.4.48.17
```

Step 2: Configure the time zone.

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

Step 3: Configure which logs to store on the appliance.

```
logging enable
logging buffered informational
```

Procedure 6 Configure device management protocols

Cisco ASDM requires that the appliance's HTTPS server be available. Be sure that the configuration includes networks where administrative staff has access the device through Cisco ASDM; the appliance can offer controlled Cisco ASDM access for a single address or management subnet.

Secure HTTP (HTTPS) and Secure Shell (SSH) are more secure replacements for the HTTP and Telnet protocols. They use Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to provide device authentication and data encryption.

Use SSH and HTTPS protocols in order to more securely manage the device. Both protocols are encrypted for privacy, and the non-secure protocols, Telnet and HTTP, are turned off.

Simple Network Management Protocol (SNMP) is enabled to allow the network infrastructure devices to be managed by a Network Management System (NMS). SNMPv2c is configured for a read-only community string.

Step 1: Allow internal administrators to remotely manage the appliance over HTTPS and SSH.

```
domain-name cisco.local
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
```

Step 2: Configure the appliance to allow SNMP polling from the NMS.

```
snmp-server host inside 10.4.48.35 community cisco
snmp-server community cisco
```

Process

Configuring Firewall High Availability

1. Configure HA on the Primary Cisco ASA
2. Configure HA on the Resilient Cisco ASA

The Cisco ASA appliances are set up as a highly available active/standby pair. Active/standby is used, rather than an active/active configuration, because this allows the same appliance to be used for firewall and VPN services (VPN functionality is disabled on the appliance in active/active configuration). In the event that the active ASA appliance fails or needs to be taken out of service for maintenance, the secondary ASA appliance assumes 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 AIP-SSMs (if the modules are installed). For failover to be enabled, the secondary ASA unit needs to be powered up and cabled to the same networks as the primary unit.

One interface on each ASA is configured as the state-synchronization interface, which the appliances use to share configuration updates, determine which device in the High Availability 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 though this interface. There can be a substantial amount of data, and it is recommended that this be a dedicated interface.

By default, the appliance 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 appliance, which minimizes the downtime a user experiences during failover. Reducing the failover timer intervals below the values in this guide is not recommended.

Procedure 1 Configure HA on the Primary Cisco ASA

This procedure describes how to configure active/standby failover. 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 Cisco ASA pair to maintain service for existing connections in the event of a failover.

Step 1: On the primary Cisco ASA, enable failover.

```
failover
```

Step 2: Configure the Cisco ASA as the primary appliance of the HA pair.

```
failover lan unit primary
```

Step 3: Configure the failover interface.

```
failover lan interface failover GigabitEthernet0/2
failover key failoverkey
failover replication http
failover link failover GigabitEthernet0/2
```

Step 4: To minimize the downtime experienced during failover, tune the failover poll timers.

```
failover polltime unit msec 200 holdtime msec 800
failover polltime interface msec 500 holdtime 5
```

Step 5: Configure the failover interface IP address.

```
failover interface ip failover 10.4.24.33 255.255.255.248 
standby 10.4.24.34
```

Step 6: Enable the failover interface.

```
interface GigabitEthernet0/2
 no shut
```

Step 7: Configure the standby IP address of the inside interface.

```
interface GigabitEthernet0/0
 ip address 10.4.24.30 255.255.255.224 standby 10.4.24.29
```

Procedure 2 Configure HA on the Resilient Cisco ASA

Step 1: On the secondary Cisco ASA, enable failover.

```
failover
```

Step 2: Configure the Cisco ASA as the secondary appliance of the HA pair.

```
failover lan unit secondary
```

Step 3: Configure the failover interface.

```
failover lan interface failover GigabitEthernet0/2
failover key failoverkey
failover replication http
failover link failover GigabitEthernet0/2
```

Step 4: To minimize the downtime experienced during failover, tune the failover poll timers.

```
failover polltime unit msec 200 holdtime msec 800
failover polltime interface msec 500 holdtime 5
```

Step 5: Configure the failover interface IP address.

```
failover interface ip failover 10.4.24.33 255.255.255.248 
standby 10.4.24.34
```

Step 6: Enable the failover interface.

```
interface GigabitEthernet0/2
 no shut
```

Step 7: To verify standby synchronization between the Cisco ASA devices, on the command-line interface of the primary appliance, issue the **show failover state** command.

```
IE-ASA5540# show failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         None
Other host -   Secondary
               Standby Ready  None

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

Process

Configuring Management DMZ

1. Configure the DMZ switch
2. Configure the Demilitarized Zone interface
3. Configure the DMZ routing
4. Configure the DMZ security policy

The firewall's demilitarized zone (DMZ) is a portion of the network where, typically, traffic to and from other parts of the network is tightly restricted. Organizations place network services in a DMZ for exposure to the Internet. These devices are typically not allowed to initiate connections to the internal network, except for specific circumstances.

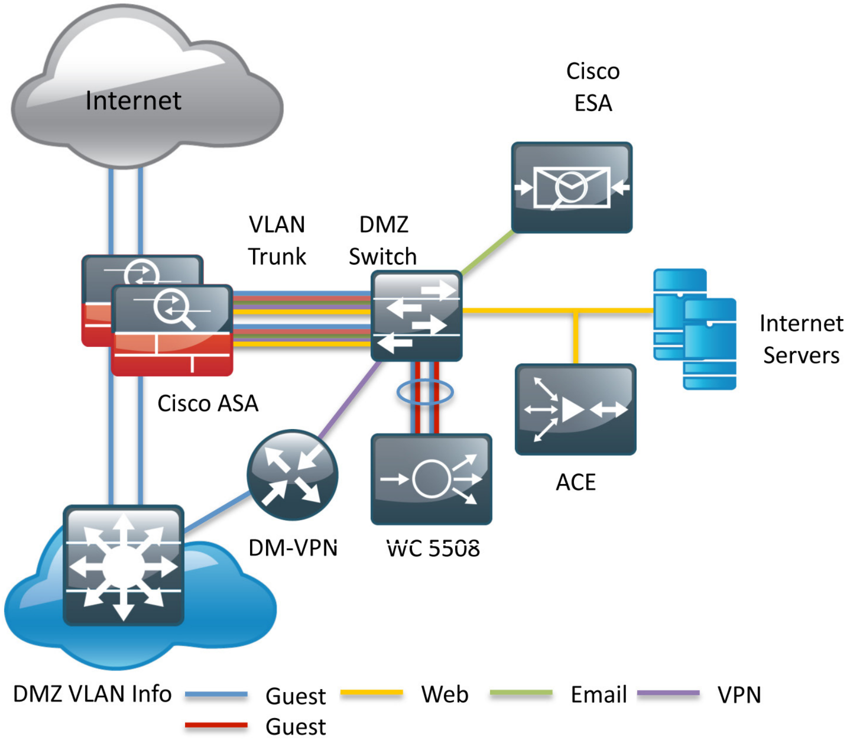
One of those special circumstances is for device management. However, the security policy on the firewall must still limit what traffic should be allowed inside from the DMZ because devices in the DMZ can be a security risk for the internal network.

To ease the configuration of the security policy, create a DMZ dedicated for the management of devices that are connected only to the DMZ or outside the firewall.

The DMZ network is connected to the appliances on the appliances' Gigabit Ethernet interface via a VLAN trunk in order to allow the greatest flexibility if new VLANs must be added in order to connect additional DMZs. The trunk connects the appliances to a 3750x switch stack that provides resiliency.

The DMZ interface on the Cisco ASA is assigned an IP address, which will be the default gateway for the DMZ network. The DMZ switch is configured to offer Layer 2 switching capability only; the DMZ switch does not have a switched virtual interface (SVI) for any VLAN, except for the management DMZ VLAN. This SVI is used for the in-band management of the switch.

Figure 8 - DMZ VLAN topology and services



Procedure 1 Configure the DMZ switch

Reader Tip

This procedure assumes that the LAN switch has already been configured following the guidance in the *Smart Business Architecture—Borderless Networks for Enterprise Organizations LAN Deployment Guide*. Only the procedures required to support the integration of the firewall into the deployment are included in this guide.

Step 1: Set the DMZ switch to be the spanning tree root for the management VLAN.

```
vlan 1123
spanning-tree vlan 1123 root primary
```

Step 2: Configure the interfaces that connect to the appliances.

```
interface GigabitEthernet1/0/24
 description IE-ASA5540a Gig0/1
!
interface GigabitEthernet1/0/24
 description IE-ASA5540b Gig0/1
!
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1123
 switchport mode trunk
 macro apply EgressQoS
 logging event link-status
 logging event trunk-status
 no shutdown
```

Step 3: Configure the switch with an IP address so that it can be managed via in-band connectivity.

```
interface Vlan1123
 description In-band management
 ip address 192.168.23.5 255.255.255.0
 no shutdown
```

Step 4: Configure the appliance as the DMZ switch's default route.

```
ip default-gateway 192.168.23.1
```

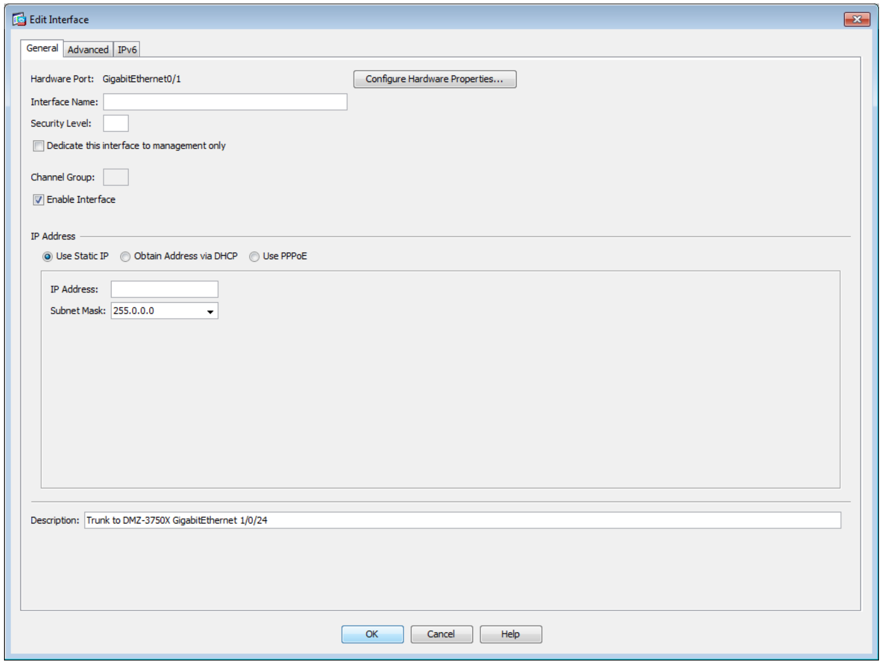
Procedure 2 Configure the Demilitarized Zone interface

Step 1: From a client on the internal network, navigate to the firewall's inside IP address, and launch the Cisco ASA Security Device Manager. (Example: https://ie-asa5540.cisco.local/)

Step 2: In **Configuration > Device Setup > Interfaces**, click the interface that is connected to the DMZ switch. (Example: GigabitEthernet0/1)

Step 3: Click **Edit**.

Step 4: In the **Edit Interface** window, select **Enable Interface**, and then click **OK**.



Hardware Port: GigabitEthernet0/1

Interface Name:

Security Level:

☐ Dedicate this interface to management only

Channel Group:

☑ Enable Interface

IP Address

● Use Static IP ○ Obtain Address via DHCP ○ Use PPPoE

IP Address:

Subnet Mask: 255.0.0.0

Description: Trunk to DMZ-3750X GigabitEthernet 1/0/24

Step 5: On the Interface pane, click **Add > Interface**.

Step 6: In the **Add Interface** window, in the **Hardware Port** list, select the interface configured in Step 1.(Example: GigabitEthernet0/1).

Step 7: In the **VLAN ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1123)

Step 8: In the **Subinterface ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1123)

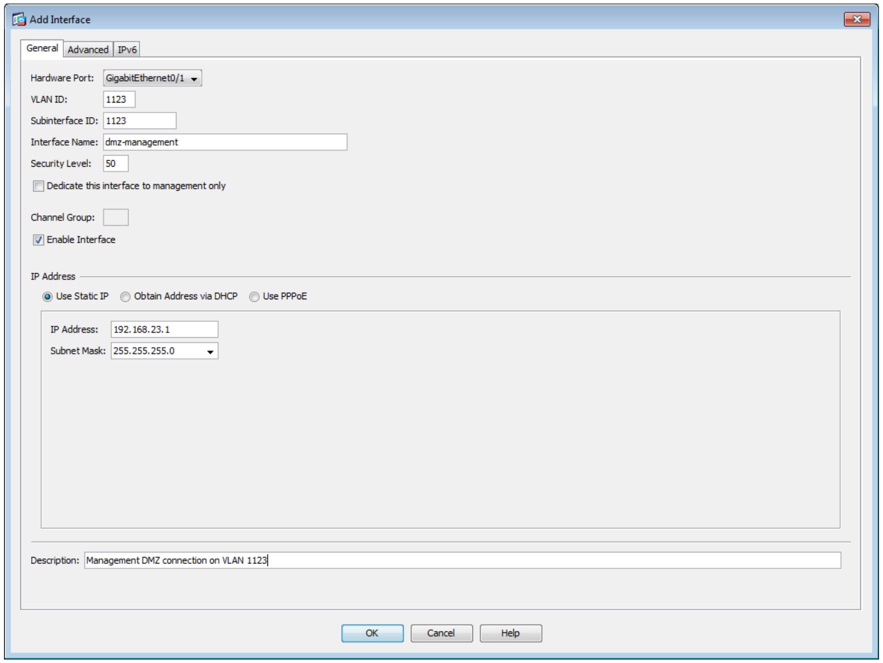
Step 9: Enter an **Interface Name**. (Example: dmz-management)

Step 10: In the **Security Level** box, enter a value of **50**.

Step 11: Enter the interface **IP Address**. (Example: 192.168.23.1)

Step 12: Enter the interface **Subnet Mask**, and then click **OK**. (Example: 255.255.255.0)

Step 13: On the Interface pane, click **Apply**.



Hardware Port: GigabitEthernet0/1

VLAN ID: 1123

Subinterface ID: 1123

Interface Name: dmz-management

Security Level: 50

☐ Dedicate this interface to management only

Channel Group:

☑ Enable Interface

IP Address

● Use Static IP ○ Obtain Address via DHCP ○ Use PPPoE

IP Address: 192.168.23.1

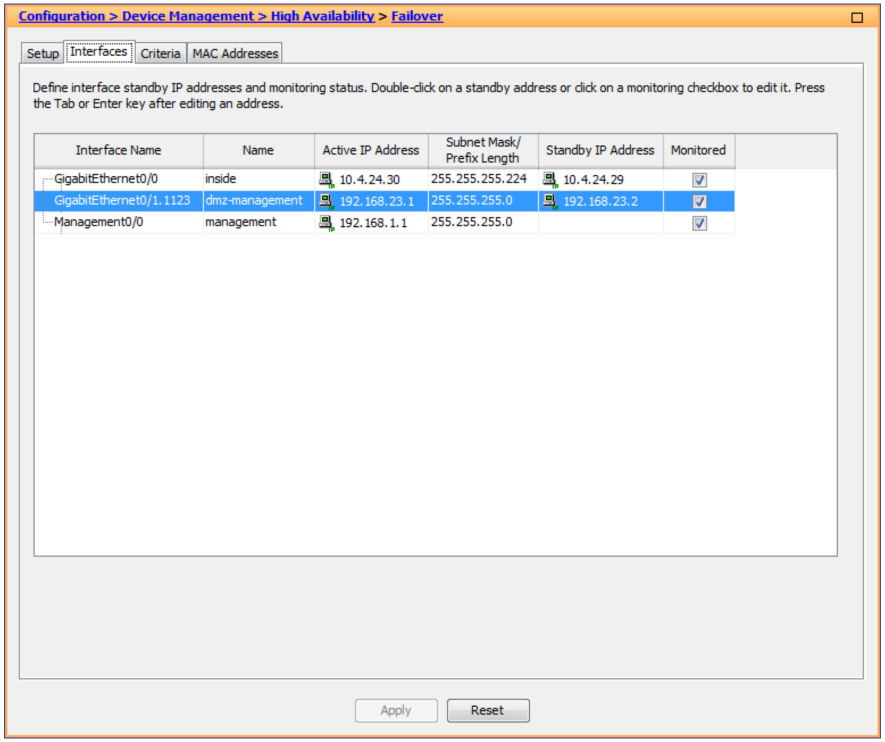
Subnet Mask: 255.255.255.0

Description: Management DMZ connection on VLAN 1123

Step 14: Navigate to **Configuration > Device Management > High Availability > Failover.**

Step 15: On the **Interfaces** tab, in the **Standby IP address** column, enter the IP address of the standby unit for the interface you just created. (Example: 192.168.23.2)

Step 16: Select **Monitored**, and then click **Apply**.



Configuration > Device Management > High Availability > Failover
Setup
Interfaces
Criteria
MAC Addresses

Define interface standby IP addresses and monitoring status. Double-click on a standby address or click on a monitoring checkbox to edit it. Press the Tab or Enter key after editing an address.

Interface Name	Name	Active IP Address	Subnet Mask/ Prefix Length	Standby IP Address	Monitored
GigabitEthernet0/0	inside	10.4.24.30	255.255.255.224	10.4.24.29	☑
GigabitEthernet0/1.1123	dmz-management	192.168.23.1	255.255.255.0	192.168.23.2	☑
Management0/0	management	192.168.1.1	255.255.255.0		☑

Procedure 3 Configure the DMZ routing

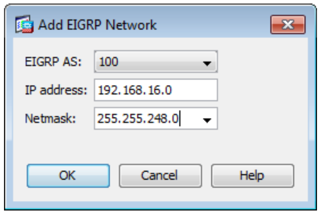
Step 1: Navigate to **Configuration** > **Device Setup** > **Routing** > **EIGRP** > **Setup**.

Step 2: On the **Networks** tab, click **Add**.

Step 3: In the **Add EIGRP Network** dialog box, in the **IP Address** box, enter the address that summarizes all DMZ networks. (Example: 192.168.16.0)

Step 4: In the **Netmask** box, enter the DMZ summary netmask, and then click **OK**. (Example: 255.255.248.0)

Step 5: On the Setup pane, click **Apply**.



EIGRP AS: 100

IP address: 192.168.16.0

Netmask: 255.255.248.0

Procedure 4 Configure the DMZ security policy

Tech Tip

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

The management DMZ provides connectivity to the internal network for devices in the DMZ and outside the firewall. This connectivity is limited to the protocols required to maintain and operate the devices.

Step 1: Navigate to **Configuration > Firewall > Access Rules**.

First, you will enable devices in the management DMZ to communicate with the internal network for management and user authentication.

Step 2: Click **Add > Add Access Rule**.

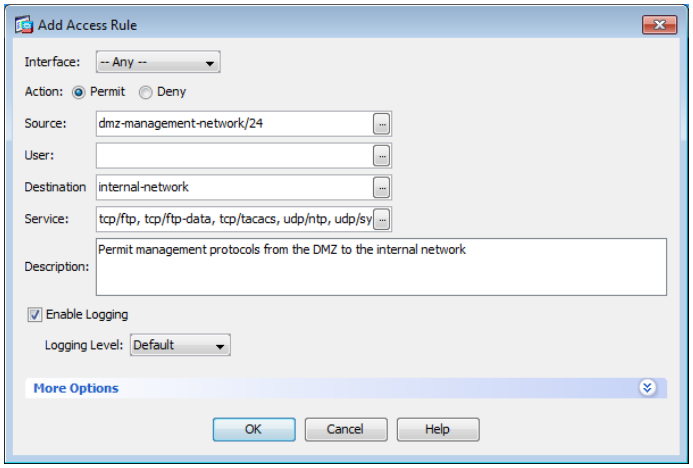
Step 3: In the **Add Access Rule** dialog box, in the **Interface** list, select **—Any—**.

Step 4: For **Action**, select **Permit**.

Step 5: In the **Source** list, select the network object automatically created for the management DMZ. (Example: dmz-management-network/24)

Step 6: In the **Destination** list, select the network object that summarizes the internal networks. (Example: internal-network)

Step 7: In the **Service** list, enter **tcp/ftp, tcp/ftp-data, tcp/tacacs, udp/ntp, udp/syslog**, and then click **OK**.



Add Access Rule

Interface: -- Any --

Action: ● Permit ○ Deny

Source: dmz-management-network/24

User:

Destination internal-network

Service: tcp/ftp, tcp/ftp-data, tcp/tacacs, udp/ntp, udp/sy

Description: Permit management protocols from the DMZ to the internal network

☑ Enable Logging

Logging Level: Default

Next, you will ease the configuration of the security policy by creating a network object that summarizes all the DMZ networks. All the DMZ networks deployed in SBA for Enterprise Organizations can be summarized as 192.168.16.0/21.

Step 8: Navigate to **Configuration > Firewall > Objects > Network Objects/Groups**.

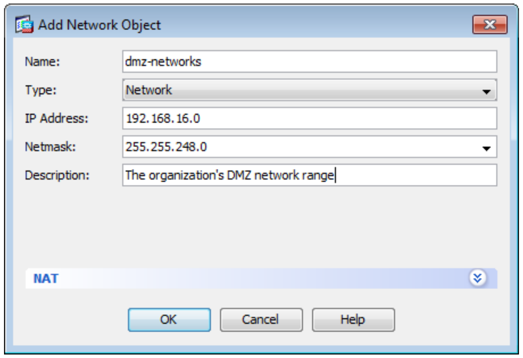
Step 9: Click **Add > Network Object**.

Step 10: In the **Add Network Object** dialog box, in the **Name box**, enter a description for the network summary. (Example: dmz-networks)

Step 11: In the **Type** list, select **Network**.

Step 12: In the **IP Address** box, enter the address that summarizes all DMZ networks. (Example: 192.168.16.0)

Step 13: In the **Netmask** box, enter the DMZ summary netmask, and then click **OK**. (Example: 255.255.248.0)



Add Network Object

Name: dmz-networks

Type: Network

IP Address: 192.168.16.0

Netmask: 255.255.248.0

Description: The organization's DMZ network range

Next, you will deny access from the DMZs to all other networks, as open access poses a security risk.

Step 14: Navigate to **Configuration > Firewall > Access Rules**.

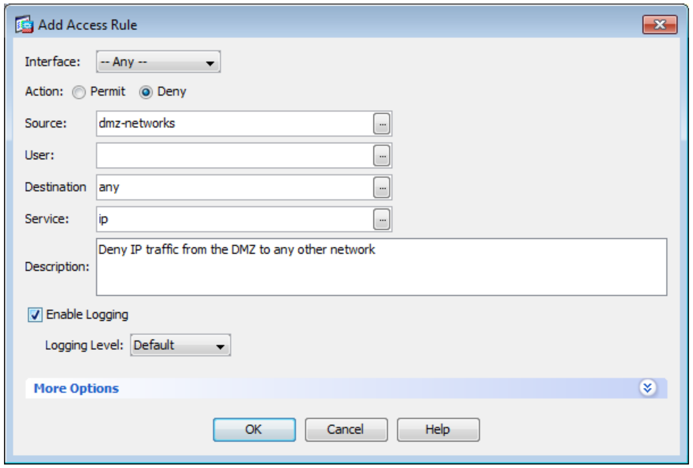
Step 15: Click **Add > Add Access Rule**.

Step 16: In the **Add Access Rule** dialog box, in the **Interface** list, select **—Any—**.

Step 17: For **Action**, select **Deny**.

Step 18: In the **Source** list, select the network object created in Step 9, and then click **OK**. (Example dmz-networks)

Step 19: On the Access Rules pane, click **Apply**.



Add Access Rule

Interface: -- Any --

Action: ○ Permit ● Deny

Source: dmz-networks

User:

Destination any

Service: ip

Description: Deny IP traffic from the DMZ to any other network

☑ Enable Logging

Logging Level: Default

Process

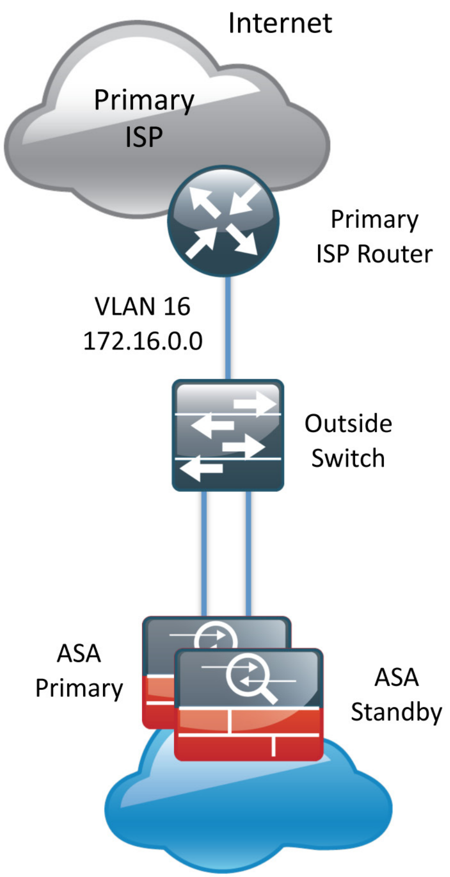
Configuring the Firewall Internet Edge

1. Configure the outside switch
2. Configure primary Internet routing
3. Configure resilient Internet routing
4. Configure address translation
5. Configure security policy

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

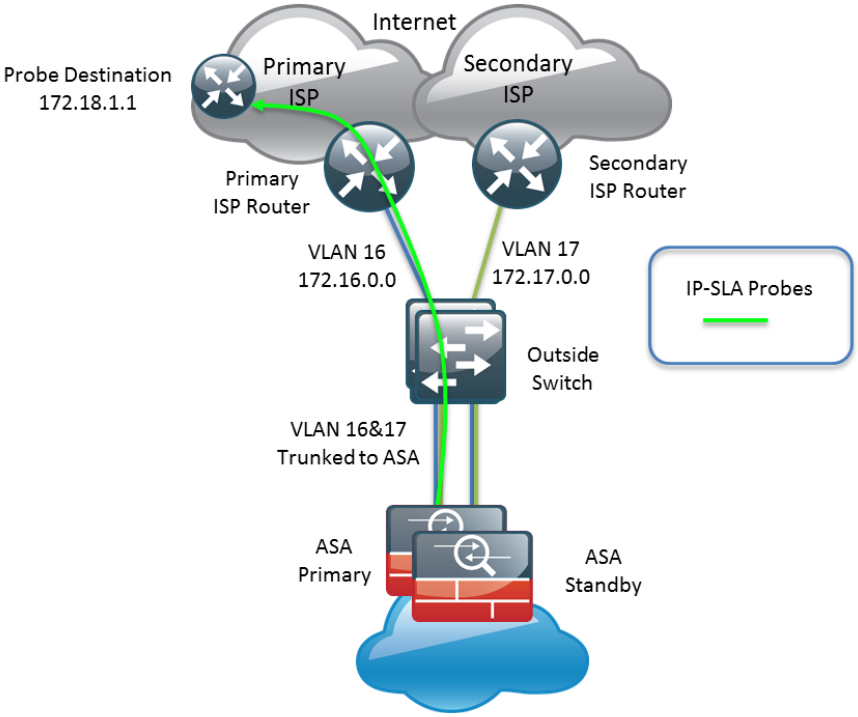
- Internet Edge 5K uses a single Internet connection via one router that carries the Internet traffic.

Figure 9 - Internet Edge 5K ISP connectivity



- Internet Edge 10K uses dual Internet connections via two routers (the primary and secondary ISP routers) that carry the Internet traffic.

Figure 10 - Internet Edge 10K ISP connectivity



An organization 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 organization 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 rule denies all traffic (i.e., "**deny ip any any**"). Whitelist policies are best suited for traffic from the Internet to services in the DMZ.

The following information is 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 in order 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 an application is blocked because of an organization's policy or because they expose the organization to malicious traffic. A blacklist policy is recognizable by the last access rule; 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 business value is very difficult to distinguish from traffic with no business value, such as malware and entertainment traffic. As an adjunct to the Cisco ASA, the Cisco IronPort Web Security Appliance (WSA) 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. IronPort WSA and IPS concepts and configuration are discussed in the IPS and Web Security modules in this document.

Procedure 1 Configure the outside switch

Reader Tip

This procedure assumes that the LAN switch has already been configured following the guidance in the *Smart Business Architecture—Borderless Networks for Enterprise Organizations LAN Deployment Guide*. Only the procedures required to support the integration of the firewall into the deployment are included in this guide.

Step 1: On the outside switch, configure the VLANs for each ISP.

```
vlan 16
 name ISP-A
!
vlan 17
 name ISP-B
!
spanning-tree vlan 16,17 root primary
```

Step 2: Configure the interfaces that are connected to the ISP routers.

```
interface GigabitEthernet1/0/23
 description ISP-A
 switchport access vlan 16
 switchport host
!
interface GigabitEthernet2/0/23
 description ISP-B
 switchport access vlan 17
 switchport host
```

Step 3: Configure the interfaces that connect to the appliances.

```
interface GigabitEthernet1/0/24
 description IE-ASA5540a Gig0/3
!
interface GigabitEthernet1/0/24
 description IE-ASA5540b Gig0/3
!
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
 switchport trunk allowed vlan 16,17
 switchport mode trunk
 logging event link-status
 logging event trunk-status
 no shutdown
```

Step 4: Configure the outside switch with an IP address.

```
interface FastEthernet0
 description DMZ-3750X Gig1/0/3
 ip address 192.168.23.6 255.255.255.0
 no shutdown
```

Step 5: Configure the firewall appliance as the default route.

```
ip default-gateway 192.168.23.1
```

Step 6: On the DMZ switch, configure the interface connected to the outside switch to be in the management DMZ.

```
interface GigabitEthernet1/0/17
 description OUT-2960Sa Fas0
!
interface GigabitEthernet2/0/17
 description OUT-2960Sa Fas0
!
interface range GigabitEthernet1/0/17, GigabitEthernet2/0/17
 switchport access vlan 1123
 switchport host
 no shutdown
```

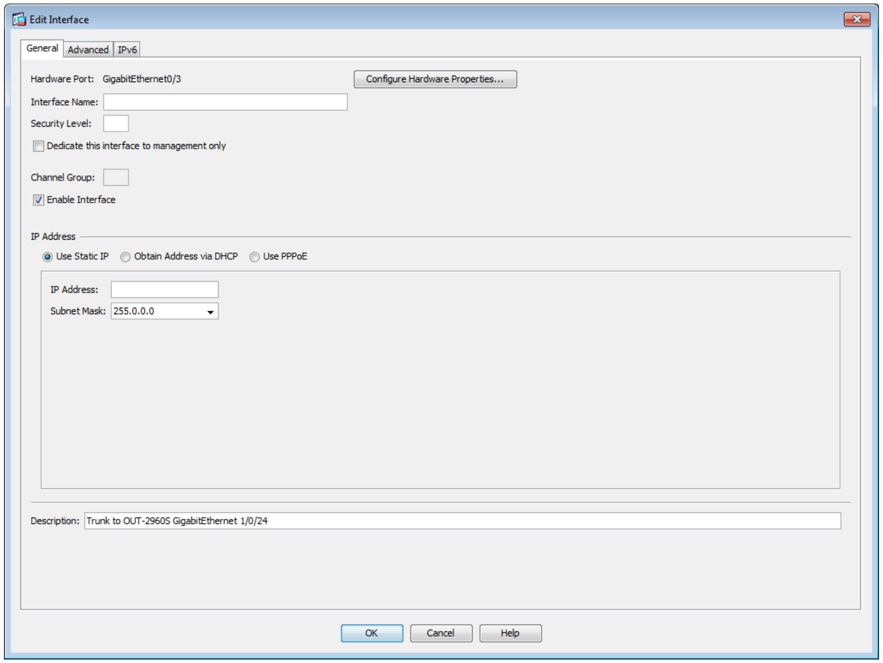
Procedure 2 Configure primary Internet routing

Step 1: From a client on the internal network, navigate to the firewall's inside IP address, and then launch the Cisco ASA Security Device Manager. (Example: https://ie-asa5540.cisco.local/)

Step 2: In **Configuration > Device Setup > Interfaces**, click the interface that is connected to the outside switch. (Example: GigabitEthernet0/3)

Step 3: Click **Edit**.

Step 4: In the **Edit Interface** dialog box, select **Enable Interface**, and then click **OK**.



Hardware Port: GigabitEthernet0/3

Interface Name:

Security Level:

☐ Dedicate this interface to management only

Channel Group:

☑ Enable Interface

● Use Static IP ○ Obtain Address via DHCP ○ Use PPPoE

IP Address:

Subnet Mask: 255.0.0.0

Description: Trunk to OUT-2960S GigabitEthernet 1/0/24

Step 5: On the Interface pane, click **Add > Interface**.

Step 6: In the **Add Interface** dialog box, in the **Hardware Port** list, select the interface configured in Step 1. (Example: GigabitEthernet0/3)

Step 7: In the **VLAN ID** box, enter the VLAN number for the primary Internet VLAN. (Example: 16)

Step 8: In the **Subinterface ID** box, enter the VLAN number for the primary Internet VLAN. (Example: 16)

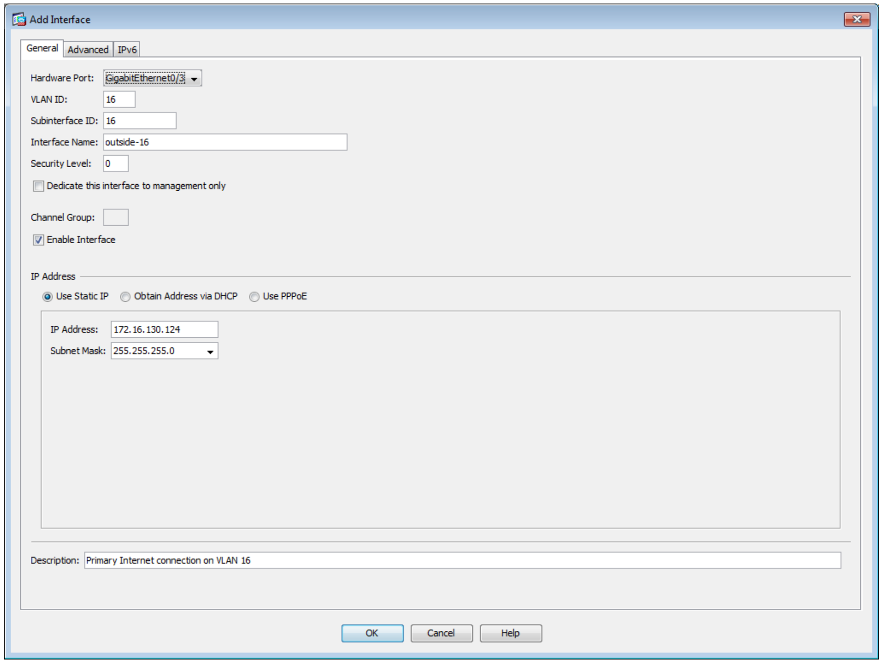
Step 9: Enter an **Interface Name**. (Example: outside-16)

Step 10: In the **Security Level** box, enter a value of **0**.

Step 11: Enter the interface **IP Address**. (Example: 172.16.130.124)

Step 12: Enter the interface **Subnet Mask**, and then click **OK**. (Example: 255.255.255.0)

Step 13: On the Interface pane, click **Apply**.



Add Interface

General | Advanced | IPv6

Hardware Port: GigabitEthernet0/3

VLAN ID: 16

Subinterface ID: 16

Interface Name: outside-16

Security Level: 0

☐ Dedicate this interface to management only

Channel Group:

☑ Enable Interface

IP Address

● Use Static IP ○ Obtain Address via DHCP ○ Use PPPoE

IP Address: 172.16.130.124

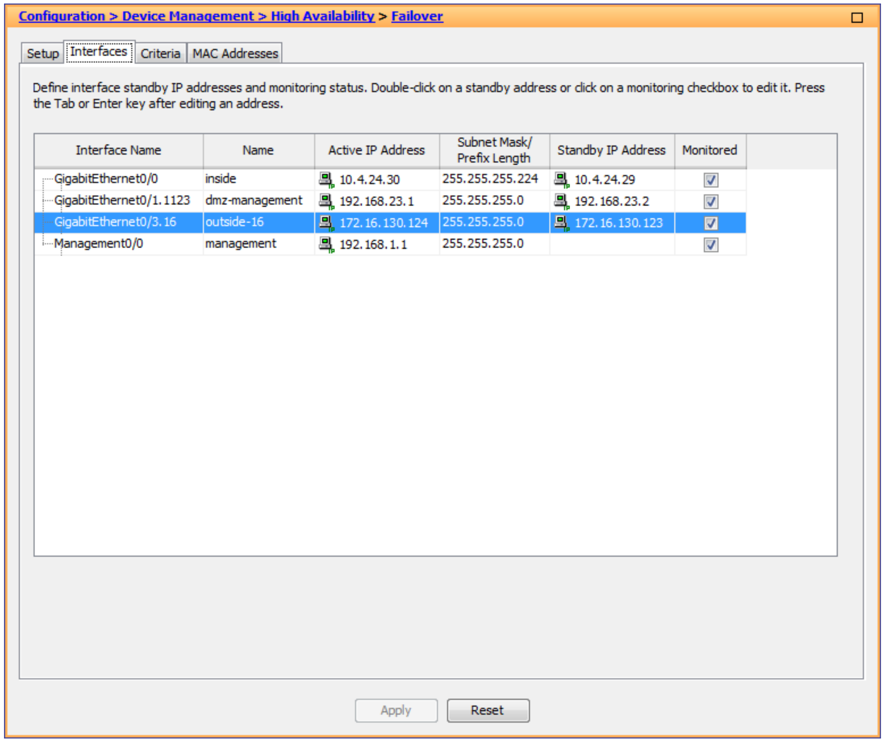
Subnet Mask: 255.255.255.0

Description: Primary Internet connection on VLAN 16

Step 14: Navigate to **Configuration > Device Management > High Availability > Failover.**

Step 15: On the **Interfaces** tab, in the **Standby IP Address** column, enter the IP address of the standby unit for the interface you just created. (Example: 172.16.130.123)

Step 16: Select **Monitored, and then click Apply**.



Configuration > Device Management > High Availability > Failover

Setup | Interfaces | Criteria | MAC Addresses

Define interface standby IP addresses and monitoring status. Double-click on a standby address or click on a monitoring checkbox to edit it. Press the Tab or Enter key after editing an address.

Interface Name	Name	Active IP Address	Subnet Mask/ Prefix Length	Standby IP Address	Monitored
GigabitEthernet0/0	inside	10.4.24.30	255.255.255.224	10.4.24.29	☑
GigabitEthernet0/1.1123	dmz-management	192.168.23.1	255.255.255.0	192.168.23.2	☑
GigabitEthernet0/3.16	outside-16	172.16.130.124	255.255.255.0	172.16.130.123	☑
Management0/0	management	192.168.1.1	255.255.255.0		☑

Next, you will create the default route to the primary Internet CPE's address.

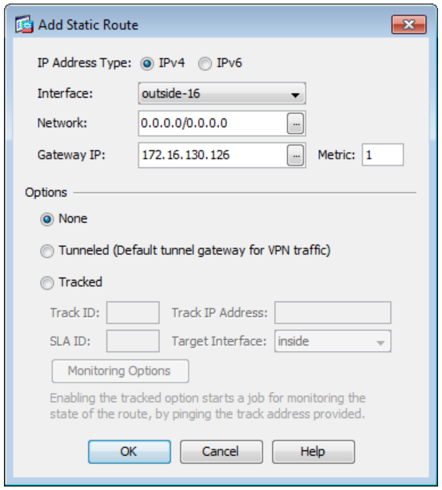
Step 17: In **Configuration > Device Setup > Routing > Static Routes**, click **Add**.

Step 18: In the **Add Static Route** dialog box, in the **Interface** list, chose the interface created in Step 6. (Example: outside-16)

Step 19: In the **Network** box, enter **0.0.0.0/0.0.0.0**.

Step 20: In the **Gateway IP** box, enter the primary Internet CPE's IP address, and then click **OK**. (Example: 172.16.130.126)

Step 21: On the Static Routes pane, click **Apply**.



Add Static Route

IP Address Type: ● IPv4 ○ IPv6

Interface: outside-16

Network: 0.0.0.0/0.0.0.0

Gateway IP: 172.16.130.126 Metric: 1

Options

● None

○ Tunneled (Default tunnel gateway for VPN traffic)

○ Tracked

Track ID: Track IP Address:

SLA ID: Target Interface: inside

Enabling the tracked option starts a job for monitoring the state of the route, by pinging the track address provided.

Procedure 3 Configure resilient Internet routing

If resilient Internet access is required, the Internet 10K design, the appliances' GigabitEthernet 0/3 is configured as a VLAN trunk to the outside switch. The VLAN trunk allows the appliance to use separate VLANs for the upstream internet routers , Internet CPE-1 and Internet CPE-2.

The primary route carries 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 to which the appliance sends ICMP probes (pings) in order to determine if the network connection is active. The target is an object on the primary service provider's network, such as an intermediate router that can be discovered with traceroute.

The tracked object should be in the primary ISP'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, including: the appliance'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 appliance should prefer the secondary ISP's route.

Step 1: Navigate to **Configuration > Device Setup > Interfaces**.

Step 2: On the Interface pane, click **Add > Interface**.

Step 3: In the **Add Interface** dialog box, in the **Hardware Port** list, choose the interface configured in Procedure 2, Step 1. (Example: GigabitEthernet0/3)

Step 4: In the **VLAN ID** box, enter the VLAN number for the resilient Internet VLAN. (Example: 17)

Step 5: In the **Subinterface ID** box, enter the VLAN number for the resilient Internet VLAN. (Example: 17)

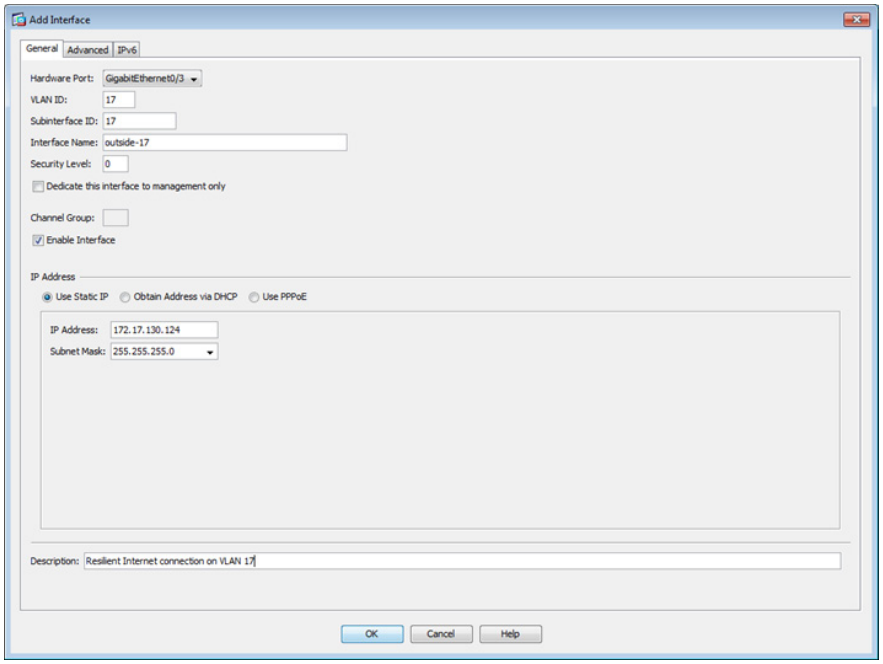
Step 6: Enter an **Interface Name**. (Example: outside-17)

Step 7: In the **Security Level** box, enter a value of **0**.

Step 8: Enter the interface **IP Address**. (Example: 172.17.130.124)

Step 9: Enter the interface **Subnet Mask**, and then click **OK**. (Example: 255.255.255.0)

Step 10: On the Interface pane, click **Apply**.



Add Interface

General | Advanced | IPv6

Hardware Port: GigabitEthernet0/3

VLAN ID: 17

Subinterface ID: 17

Interface Name: outside-17

Security Level: 0

☐ Dedicate this interface to management only

Channel Group:

☑ Enable Interface

IP Address

● Use Static IP ○ Obtain Address via DHCP ○ Use PPPoE

IP Address: 172.17.130.124

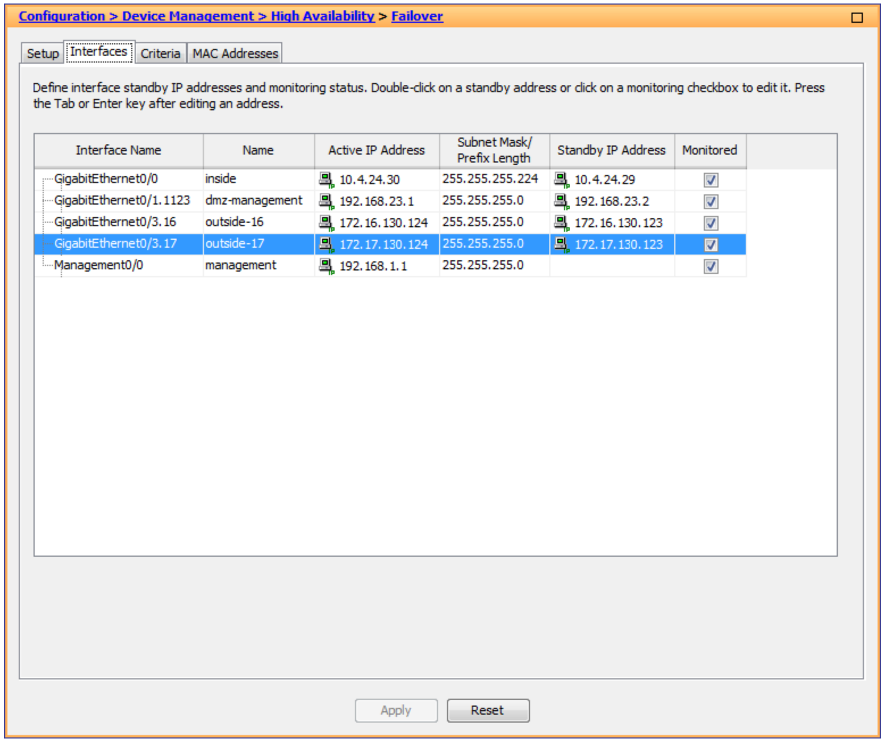
Subnet Mask: 255.255.255.0

Description: Resilient Internet connection on VLAN 17

Step 11: Navigate to **Configuration > Device Management > High Availability > Failover.**

Step 12: On the **Interfaces** tab, in the **Standby IP Address** column, enter the IP address of the standby unit for the interface you just created. (Example: 172.17.130.123)

Step 13: Select **Monitored**, and then click **Apply**.



Configuration > Device Management > High Availability > Failover

Setup | Interfaces | Criteria | MAC Addresses

Define interface standby IP addresses and monitoring status. Double-click on a standby address or click on a monitoring checkbox to edit it. Press the Tab or Enter key after editing an address.

Interface Name	Name	Active IP Address	Subnet Mask/ Prefix Length	Standby IP Address	Monitored
GigabitEthernet0/0	inside	10.4.24.30	255.255.255.224	10.4.24.29	☑
GigabitEthernet0/1.1123	dmz-management	192.168.23.1	255.255.255.0	192.168.23.2	☑
GigabitEthernet0/3.16	outside-16	172.16.130.124	255.255.255.0	172.16.130.123	☑
GigabitEthernet0/3.17	outside-17	172.17.130.124	255.255.255.0	172.17.130.123	☑
Management0/0	management	192.168.1.1	255.255.255.0		☑

Next, you will edit the default route to the primary Internet CPE's address.

Step 14: Navigate to **Configuration > Device Setup > Routing > Static Routes.**

Step 15: Select the default route created in Procedure 2, and click **Edit**.

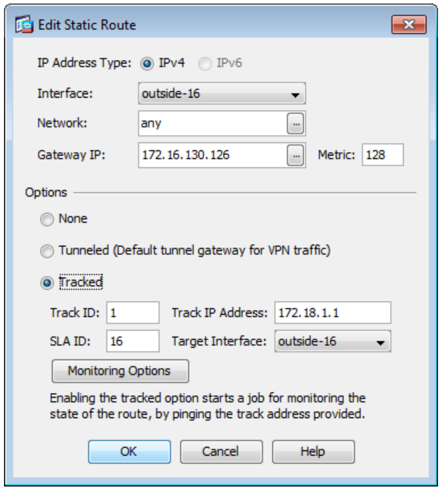
Step 16: In the **Edit Static Route** dialog box, in the **Options** pane, select **Tracked**.

Step 17: In the **Track ID** box, enter **1**.

Step 18: In the **Track IP Address** box, enter an IP address in the ISP's cloud. (Example: 172.18.1.1)

Step 19: In the **SLA ID** box, enter **16**.

Step 20: In the **Target Interface** list, select the primary Internet connection interface, and then click **OK**. (Example: outside-16)



Edit Static Route

IP Address Type: ● IPv4 ○ IPv6

Interface: outside-16

Network: any

Gateway IP: 172.16.130.126 Metric: 128

Options

○ None

○ Tunneled (Default tunnel gateway for VPN traffic)

● Tracked

Track ID: 1 Track IP Address: 172.18.1.1

SLA ID: 16 Target Interface: outside-16

Enabling the tracked option starts a job for monitoring the state of the route, by pinging the track address provided.

Step 21: On the **Information** dialog box, click **OK**.

Next, you will create the secondary default route to the resilient Internet CPE's address.

Step 22: In **Configuration > Device Setup > Routing > Static Routes**, click **Add**.

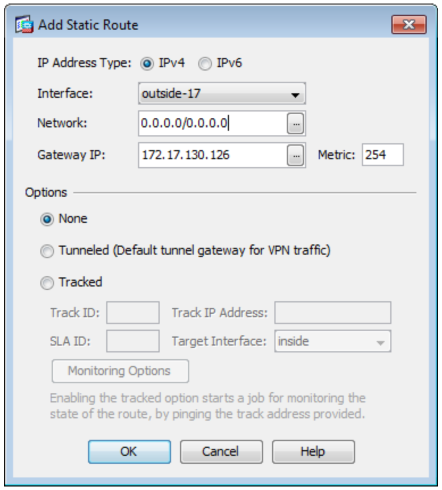
Step 23: In the **Add Static Route** dialog box, in the **Interface** list, select the resilient Internet connection interface created in Step 6. (Example: outside-17)

Step 24: In the **Network** box, enter **0.0.0.0/0.0.0.0**.

Step 25: In the **Gateway IP** box, enter the primary Internet CPE's IP address. (Example: 172.17.130.126)

Step 26: In the **Metric** box, enter **254**, and then click **OK**.

Step 27: On the Static Routes pane, click **Apply**.



Add Static Route

IP Address Type: ● IPv4 ○ IPv6

Interface: outside-17

Network: 0.0.0.0/0.0.0.0

Gateway IP: 172.17.130.126 Metric: 254

Options

● None

○ Tunneled (Default tunnel gateway for VPN traffic)

○ Tracked

Track ID: Track IP Address:

SLA ID: Target Interface: inside

Enabling the tracked option starts a job for monitoring the state of the route, by pinging the track address provided.

Next, you will add a host route for the tracked object via the Internet-CPE-1 address. This assures that probes to the tracked object will always use the primary ISP connection.

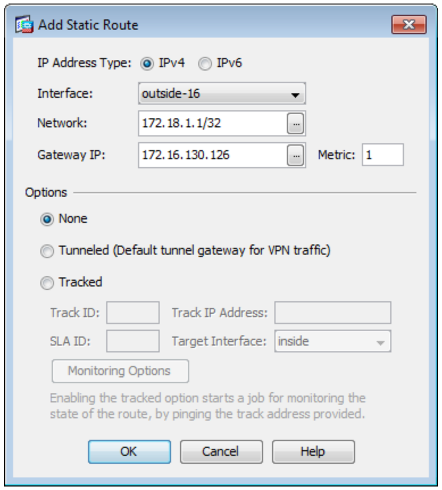
Step 28: In **Configuration > Device Setup > Routing > Static Routes**, click **Add**.

Step 29: In the **Add Static Route** dialog box, in the **Interface** list, select the primary Internet connection interface created in Procedure 2. (Example: outside-16)

Step 30: In the **Network** box, enter the IP address used for tracking in the primary default route. (Example: 172.18.1.1/32)

Step 31: In the **Gateway IP** box, enter the primary Internet CPE's IP address, and then click **OK**. (Example: 172.16.130.126)

Step 32: On the Static Routes pane, click **Apply**.



Add Static Route

IP Address Type: ● IPv4 ○ IPv6

Interface: outside-16

Network: 172.18.1.1/32

Gateway IP: 172.16.130.126 Metric: 1

Options

● None

○ Tunneled (Default tunnel gateway for VPN traffic)

○ Tracked

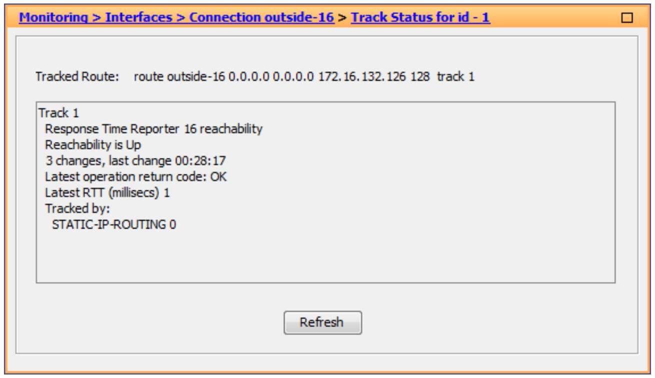
Track ID: Track IP Address:

SLA ID: Target Interface: inside

Enabling the tracked option starts a job for monitoring the state of the route, by pinging the track address provided.

Step 33: In Cisco ASDM, refresh the configuration.

Step 34: You can monitor the reachability of the tracked object by navigating to **Monitoring > Interfaces > Connection outside-16 > Track Status for id-1**.



Monitoring > Interfaces > Connection outside-16 > Track Status for id - 1

Tracked Route: route outside-16 0.0.0.0 0.0.0.0 172.16.132.126 128 track 1

```
Track 1
 Response Time Reporter 16 reachability
 Reachability is Up
 3 changes, last change 00:28:17
 Latest operation return code: OK
 Latest RTT (millisecs) 1
 Tracked by:
  STATIC-IP-ROUTING 0
```

Procedure 4 Configure address translation

Prior to completing this procedure, access to the Internet from within the inside network is not possible. This procedure 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 appliances 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.

Tech Tip

As the address translation configuration described in this portion of the document is applied, the appliance enables its default access rule set. Review the expected traffic carefully; if any traffic 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 there are some additional steps for configuring both outside interfaces in the Internet Edge 10K design.

Step 1: Navigate to **Configuration > Firewall > Objects > Network Objects/Groups**.

Step 2: Click **Add > Network Object**.

Step 3: In the **Add Network Object** dialog box, in the **Name box**, enter a description for the address translation. (Example: internal-network-ISPa)

Step 4: In the **Type** list, select **Network**.

Step 5: In the **IP Address** box, enter the address that summarizes all internal networks. (Example: 10.4.0.0)

Step 6: In the **Netmask** box, enter the internal summary netmask. (Example: 255.254.0.0)

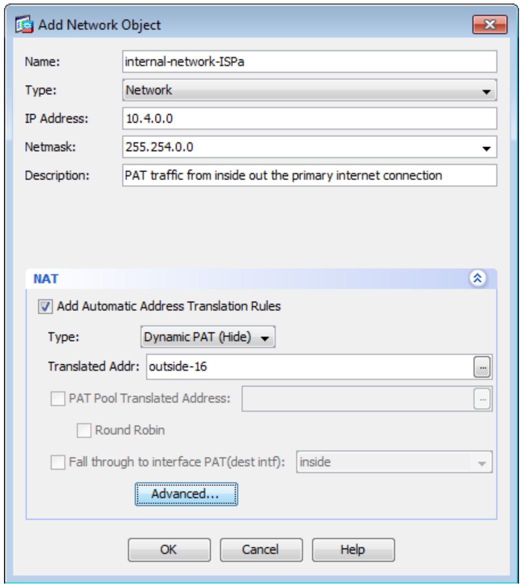
Step 7: Click the two down arrows. The **NAT** pane expands.

Step 8: Select **Add Automatic Address Translation Rules**.

Step 9: In the **Type** list, select **Dynamic PAT (Hide).**

Step 10: In the **Translated Addr.** box, enter the name of the primary Internet connection interface, and then click **OK**. (Example: outside-16)

Step 11: On the Network Objects/Groups pane, click **Apply**.



Add Network Object

Name: internal-network-ISPa

Type: Network

IP Address: 10.4.0.0

Netmask: 255.254.0.0

Description: PAT traffic from inside out the primary internet connection

NAT

☑ Add Automatic Address Translation Rules

Type: Dynamic PAT (Hide)

Translated Addr: outside-16

□ PAT Pool Translated Address:

□ Round Robin

□ Fall through to interface PAT(dest intf): inside

Step 12: If you are using the Internet Edge 10k design, which has a resilient internet connection, repeat Step 1 - Step 11 for the resilient Internet connection.

If you are using the Internet Edge 5k design, advance to the next procedure.

Procedure 5 Configure security policy

The security policy is typically configured so that internal network traffic to the DMZs or Internet is blocked only for high-risk services; all other access is allowed.

Telnet is an example of a network service that is high-risk, because it carries all of its data unencrypted. This poses a risk because hosts that can intercept the data can potentially view sensitive data.

Step 1: Navigate to **Configuration > Firewall > Access Rules**.

First, you will add a rule to deny the internal network from sending outbound Telnet requests.

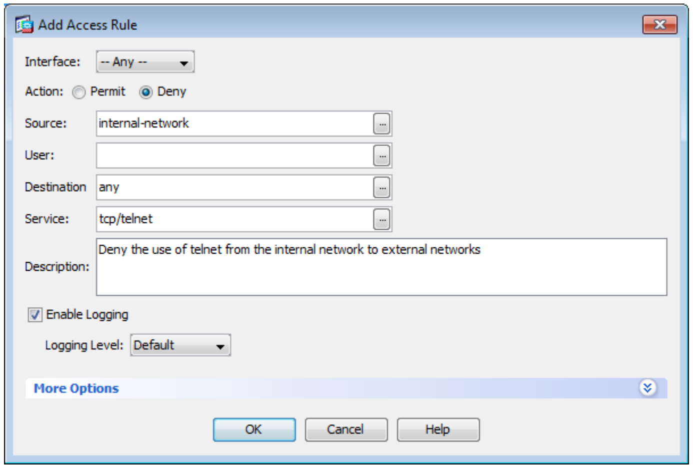
Step 2: Click **Add > Add Access Rule**.

Step 3: In the **Add Access Rule** dialog box, in the **Interface** list, select **—Any—**.

Step 4: For **Action**, select **Deny**.

Step 5: In the **Source** list, select the network object that summarizes the internal networks. (Example: internal-network)

Step 6: In the **Service** list, enter **tcp/telnet**, and then click **OK**.



Add Access Rule

Interface: -- Any --

Action: ○ Permit ● Deny

Source: internal-network

User:

Destination any

Service: tcp/telnet

Description: Deny the use of telnet from the internal network to external networks

☑ Enable Logging

Logging Level: Default

Next, you will add a rule to permit all remaining traffic from the internal network.

Step 7: Click **Add > Add Access Rule**.

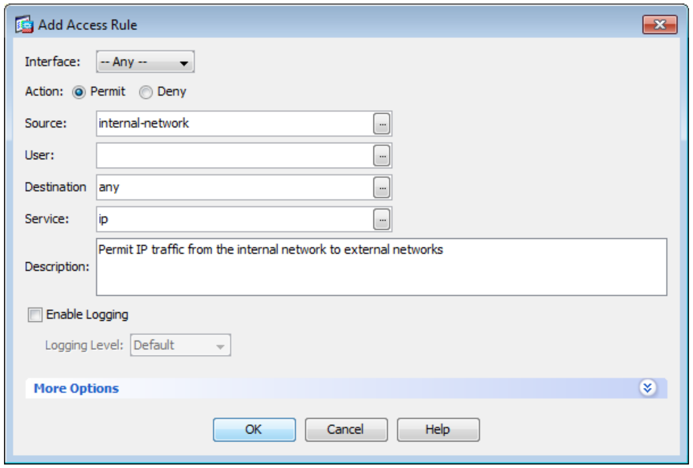
Step 8: In the **Add Access Rule** dialog box, in the **Interface** list, select **—Any—**.

Step 9: For **Action**, select **Permit**.

Step 10: In the **Source** list, select the network object that summarizes the internal networks. . (Example: internal-network)

Step 11: Clear **Enable Logging**, and then click **OK**

Step 12: On the Access Rules pane, click **Apply.**



Interface: -- Any --

Action: ● Permit ○ Deny

Source: internal-network

User:

Destination any

Service: ip

Description: Permit IP traffic from the internal network to external networks

□ Enable Logging

Logging Level: Default

Process

Configuring the Web DMZ

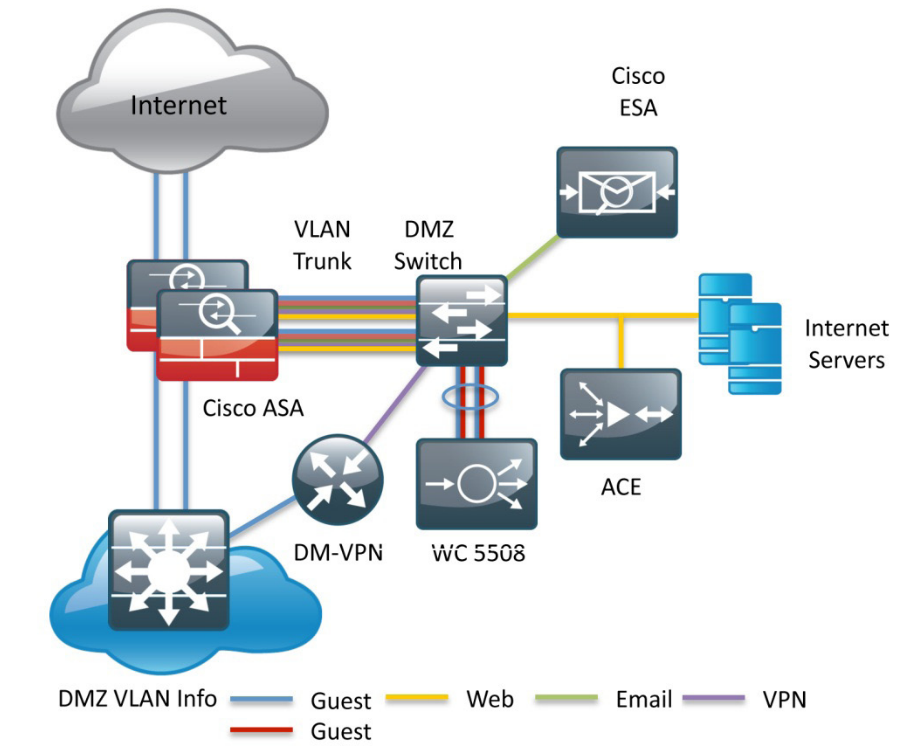
1. Configure the DMZ switch
2. Configure DMZ interface
3. Configure Network Address Translation
4. Configure security policy

The firewall's demilitarized zone (DMZ) is a portion of the network where, typically, traffic to and from other parts of the network is tightly restricted. Organizations 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.

In this process a DMZ is configured to enable you to host Internet-accessible web servers to be on site.

The DMZ network is connected to the appliances on the appliances' GigabitEthernet interface via a VLAN trunk in order to allow the greatest flexibility if new VLANs must be added to connect additional DMZs. The trunk connects the appliances to a 3750x access-switch stack in order to provide resiliency. The DMZ VLAN interfaces on the Cisco ASA are each assigned an IP address that is 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, except for one VLAN interface with an IP address for management of the switch.

Figure 11 - 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 because 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 improves performance and reduces load on network devices.

Tech Tip

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

Procedure 1 Configure the DMZ switch

Reader Tip

This procedure assumes that the LAN switch has already been configured following the guidance in the *Smart Business Architecture—Borderless Networks for Enterprise Organizations LAN Deployment Guide*. Only the procedures required to support the integration of the firewall into the deployment are included in this guide. .

Step 1: Set the DMZ switch to be the spanning tree root for the VLAN that contains the WLCs.

```
vlan 1116
spanning-tree vlan 1116 root primary
```

Step 2: Configure the interfaces that connect to the appliances.

```
interface GigabitEthernet1/0/24
 description IE-ASA5540a Gig0/1
!
interface GigabitEthernet1/0/24
 description IE-ASA5540b Gig0/1
!
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan add 1116
 switchport mode trunk
 macro apply EgressQoS
 logging event link-status
 logging event trunk-status
 no shutdown
```

Step 3: Configure the interfaces that are connected to the web server.

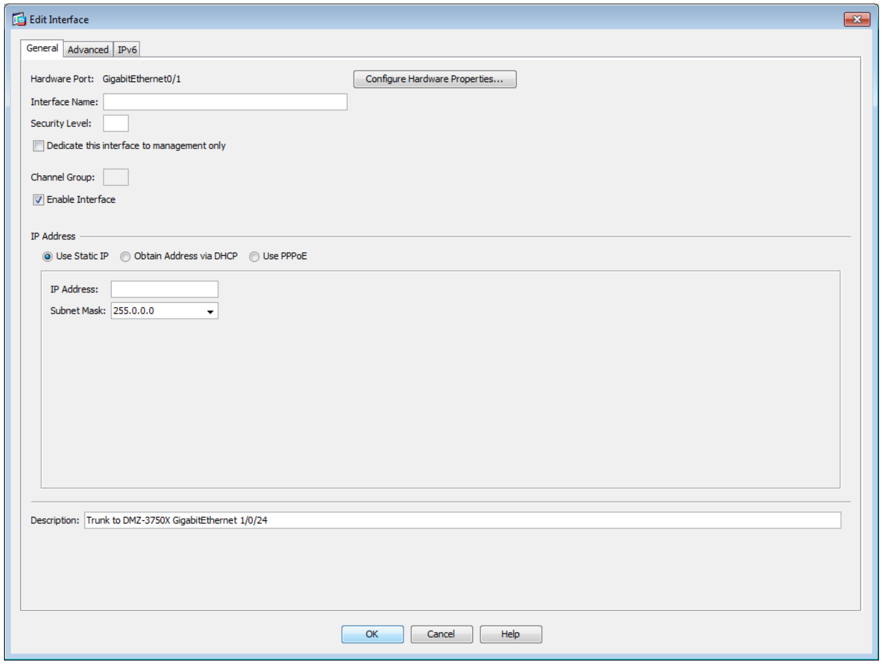
```
interface GigabitEthernet1/0/2
 description Webserver
 switchport access vlan 1116
 switchport host
 macro apply EgressQoS
 logging event link-status
 no shutdown
```

Procedure 2 Configure DMZ interface

Step 1: In **Configuration > Device Setup > Interfaces**, click the interface that is connected to the DMZ switch. (Example: GigabitEthernet0/1)

Step 2: Click **Edit**.

Step 3: In the **Edit Interface** dialog box, select **Enable Interface**, and then click **OK**.



Edit Interface

General | Advanced | IPv6

Hardware Port: GigabitEthernet0/1

Interface Name:

Security Level:

□ Dedicate this interface to management only

Channel Group:

☑ Enable Interface

IP Address

● Use Static IP ○ Obtain Address via DHCP ○ Use PPPoE

IP Address:

Subnet Mask: 255.0.0.0

Description: Trunk to DMZ-3750X GigabitEthernet 1/0/24

Step 4: On the Interface pane, click **Add > Interface**.

Step 5: In the **Add Interface** dialog box, in the **Hardware Port** list, choose the interface configured in Step 1.(Example: GigabitEthernet0/1)

Step 6: In the **VLAN ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1116)

Step 7: In the **Subinterface ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1116)

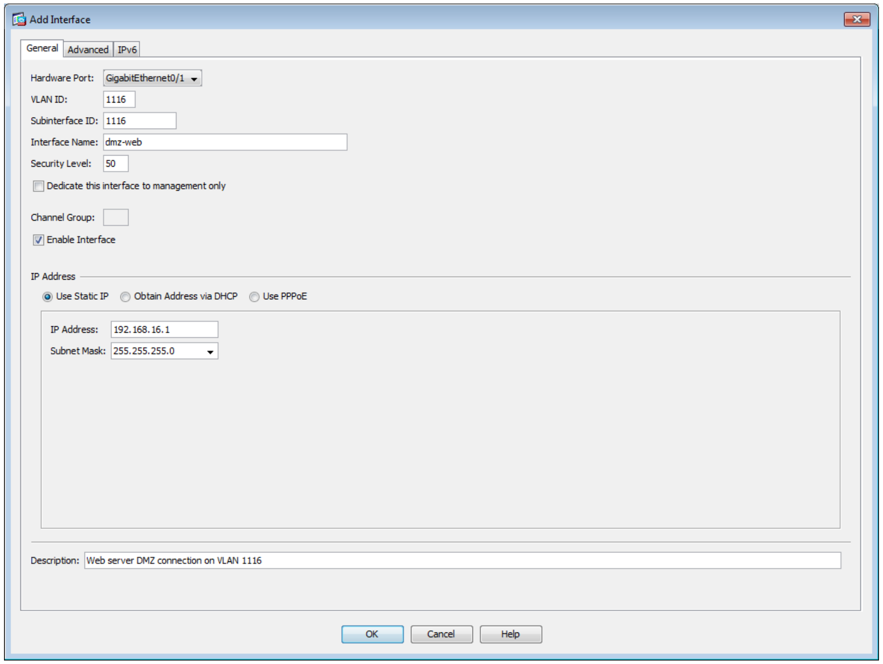
Step 8: Enter an **Interface Name**. (Example: dmz-web)

Step 9: In the **Security Level** box, enter a value of **50**.

Step 10: Enter the interface **IP Address**. (Example: 192.168.16.1)

Step 11: Enter the interface **Subnet Mask**, and then click **OK**. (Example: 255.255.255.0)

Step 12: On the Interface pane, click **Apply**.



Add Interface

General | Advanced | IPv6

Hardware Port: GigabitEthernet0/1

VLAN ID: 1116

Subinterface ID: 1116

Interface Name: dmz-web

Security Level: 50

□ Dedicate this interface to management only

Channel Group:

☑ Enable Interface

IP Address

● Use Static IP ○ Obtain Address via DHCP ○ Use PPPoE

IP Address: 192.168.16.1

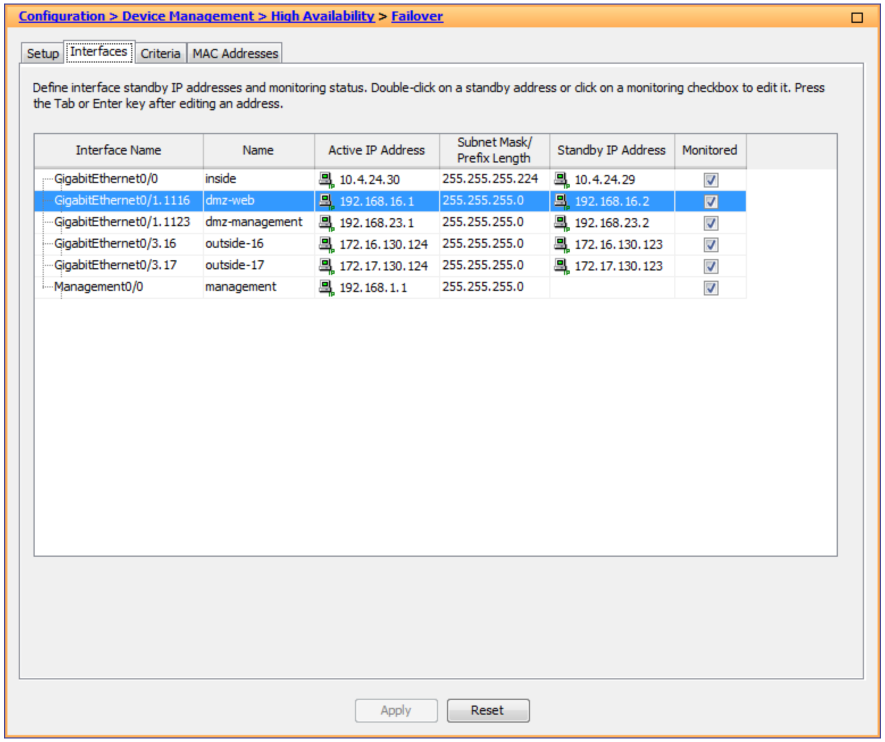
Subnet Mask: 255.255.255.0

Description: Web server DMZ connection on VLAN 1116

Step 13: Navigate to **Configuration > Device Management > High Availability > Failover.**

Step 14: On the **Interfaces** tab, in the **Standby IP address** column, enter the IP address of the standby unit for the interface you just created. (Example: 192.168.16.2)

Step 15: Select **Monitored, and then click Apply**.



Configuration > Device Management > High Availability > Failover
Setup
Interfaces
Criteria
MAC Addresses

Define interface standby IP addresses and monitoring status. Double-click on a standby address or click on a monitoring checkbox to edit it. Press the Tab or Enter key after editing an address.

Interface Name	Name	Active IP Address	Subnet Mask/ Prefix Length	Standby IP Address	Monitored
GigabitEthernet0/0	inside	10.4.24.30	255.255.255.224	10.4.24.29	☑
GigabitEthernet0/1.1116	dmz-web	192.168.16.1	255.255.255.0	192.168.16.2	☑
GigabitEthernet0/1.1123	dmz-management	192.168.23.1	255.255.255.0	192.168.23.2	☑
GigabitEthernet0/3.16	outside-16	172.16.130.124	255.255.255.0	172.16.130.123	☑
GigabitEthernet0/3.17	outside-17	172.17.130.124	255.255.255.0	172.17.130.123	☑
Management0/0	management	192.168.1.1	255.255.255.0		☑

Procedure 3 Configure Network Address Translation

The DMZ network uses private network (RFC 1918) addressing that is not Internet-routable, so the firewall must translate the DMZ address of the web server to an outside public address. If there is a resilient Internet connection, the web server can have an address translation for each ISP. This resilient configuration, shown here for completeness, relies on the modification of DNS records in order to point incoming requests to the resilient web server address when the primary Internet connection is unavailable.

The example DMZ address to public IP address mapping is shown in the following table.

Table 4 - DMZ address mapping

Web server DMZ address	Web server public address (externally routable after NAT)
192.168.16.100	172.16.130.100 (ISP-A)
	172.17.130.100 (ISP-B)

Step 1: Navigate to **Configuration > Firewall > Objects > Network Objects/Groups**.

First, you will add a network object for the web server's IP address on the primary Internet connection.

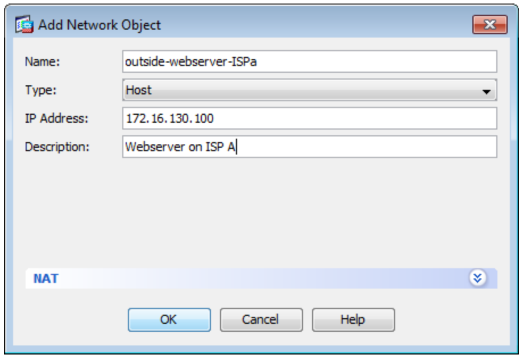
Step 2: Click **Add > Network Object**.

Step 3: On the **Add Network Object** dialog box, in the **Name box**, enter a description for the web server's public IP address. (Example: outside-webserver-ISPa)

Step 4: In the **Type** list, select **Host**.

Step 5: In the **IP Address** box, enter the web server's public IP address, and then click **OK**. (Example: 172.16.130.100)

Step 6: On the Network Objects/Groups pane, click **Apply**.



Name: outside-webserver-ISPa
Type: Host
IP Address: 172.16.130.100
Description: Webserver on ISP A

Next, you will add a network object for the private DMZ address of the web server.

Step 7: Click **Add > Network Object**.

Step 8: On the **Add Network Object** dialog box, in the **Name box**, enter a description for the web server's private DMZ IP address. (Example: dmz-webserver-ISPa)

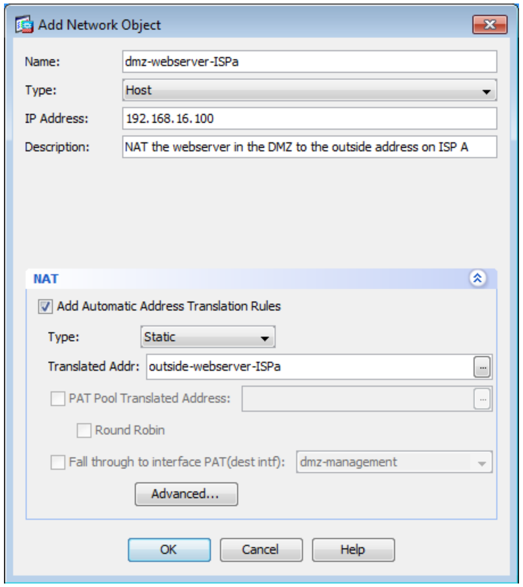
Step 9: In the **Type** list, select **Host**.

Step 10: In the **IP Address** box, enter the web server's private DMZ IP address. (Example: 192.168.16.100)

Step 11: Click the two down arrows. The **NAT** pane expands.

Step 12: Select **Add Automatic Address Translation Rules**.

Step 13: In the **Translated Addr** list, select the network object created in Step 2. (Example: outside-webserver-ISPa)

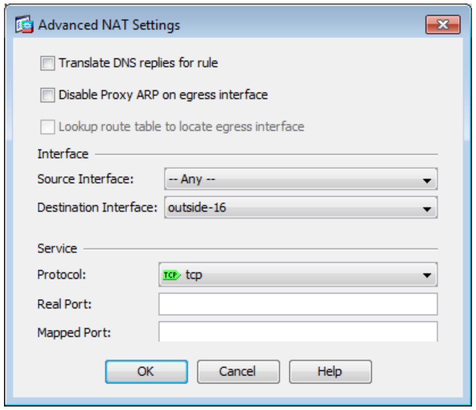


Name: dmz-webserver-ISPa
Type: Host
IP Address: 192.168.16.100
Description: NAT the webserver in the DMZ to the outside address on ISP A

☑ Add Automatic Address Translation Rules
Type: Static
Translated Addr: outside-webserver-ISPa
□ PAT Pool Translated Address:
□ Round Robin
□ Fall through to interface PAT(dest intf): dmz-management

Step 14: Click **Advanced**.

Step 15: In the **Advanced NAT Settings** dialog box, in the **Destination Interface** list, select the interface name for the primary Internet connection, and then click **OK**. (Example: outside-16)



Advanced NAT Settings

☐ Translate DNS replies for rule

☐ Disable Proxy ARP on egress interface

☐ Lookup route table to locate egress interface

Interface

Source Interface: -- Any --

Destination Interface: outside-16

Service

Protocol: tcp

Real Port:

Mapped Port:

Step 16: In the **Add Network Object** dialog box, click **OK**.

Step 17: On the Network Objects/Groups pane, click **Apply**.

Step 18: If you are using the Internet Edge 10k design, which has a resilient internet connection, repeat this procedure for the resilient Internet connection.

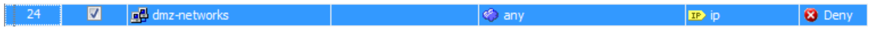
If you are using the Internet Edge 5k design, advance to the next procedure.

Procedure 4 Configure security policy

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: Navigate to **Configuration > Firewall > Access Rules**.

Step 2: Click the rule that denies traffic from the DMZ toward other networks.



24 ☑ dmz-networks any ip Deny

Next, you will insert a new rule above the rule you selected.

Step 3: Click **Add > Insert**.

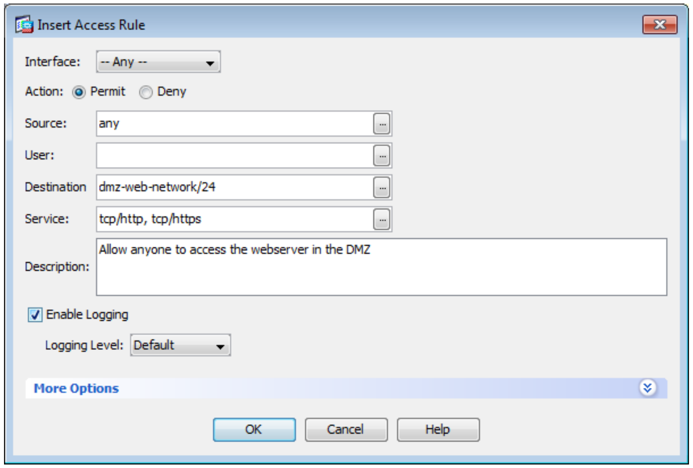
Step 4: In the **Internet Access Rule** dialog box, in the **Interface** list, select **—Any—**.

Step 5: For **Action**, select **Permit**.

Step 6: In the **Destination** list, select the network object automatically created for the web DMZ. (Example: dmz-web-network/24)

Step 7: In the **Service** list, enter **tcp/http, tcp/https**, and then click **OK**.

Step 8: On the Access Rules pane, click **Apply**.


Insert Access Rule

Interface: -- Any --

Action: ● Permit ○ Deny

Source: any

User:

Destination dmz-web-network/24

Service: tcp/http, tcp/https

Description: Allow anyone to access the webserver in the DMZ

☑ Enable Logging

Logging Level: Default

Firewall Summary

This section described concepts and configuration for:

- Routing to the Internet.
- Firewall management and monitoring.
- Inside-network NAT and firewall policy recommendations.
- DMZ Configuration for internet accessible web servers.

The section finished with a discussion and configuration of active/standby failover for Cisco ASA firewalls.

Notes

Intrusion Prevention

Business Overview

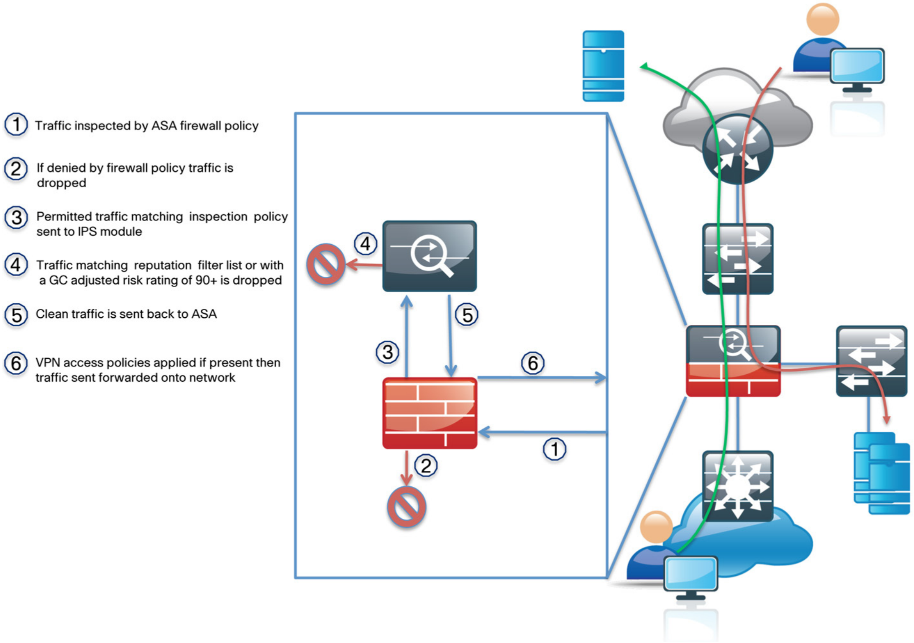
Internet services have become a key part of day-to-day operations for many organizations today. Providing secure Internet access, while preventing malicious content from entering an organization is critical to maintaining employee productivity. In addition to client access to the Internet, organizations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

Technology Overview

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

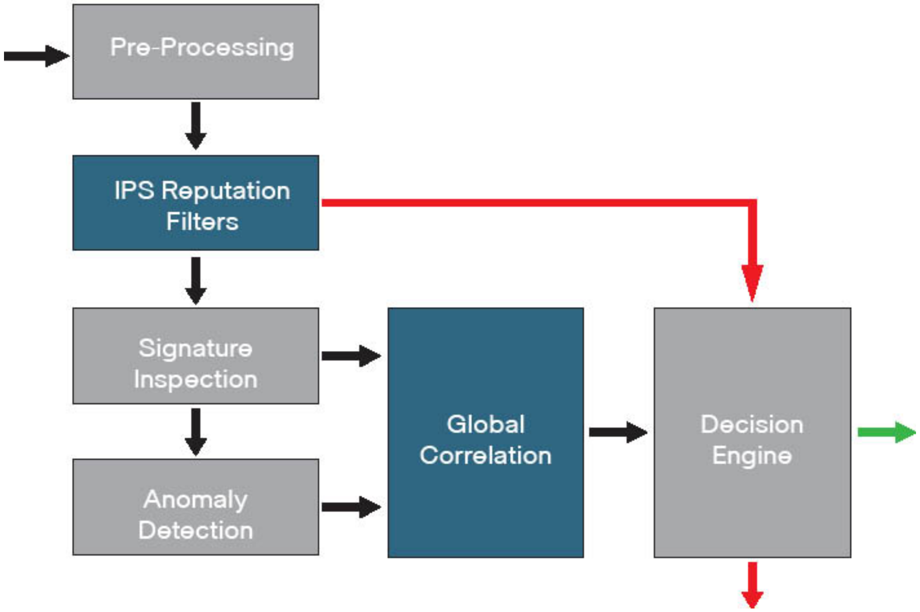
This design employs the Cisco Adaptive Inspection Prevention Security Service Module (AIP-SSM) for IPS services in the Internet Edge Cisco ASA 5500 series firewalls. The design offers several options that are based on the performance requirements of the organization. For the Internet Edge 5K, Cisco ASA 5520 with AIP-SSM-20 is recommended. The AIP-SSM-20 supports up to 375 Mbps of traffic for IPS inspection. For larger networks, such as the Internet Edge 10K design, the Cisco ASA 5540 with AIP-SSM-40 supports 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 12 - Packet flow through an ASA and AIP-SSM


1 Traffic inspected by ASA firewall policy
2 If denied by firewall policy traffic is dropped
3 Permitted traffic matching inspection policy sent to IPS module
4 Traffic matching reputation filter list or with a GC adjusted risk rating of 90+ is dropped
5 Clean traffic is sent back to ASA
6 VPN access policies applied if present then traffic sent forwarded onto network
4
5
3
6
1
2

AIP-SSMs integrated into the appliance rely on the appliance for High Availability services. The appliances in the Internet Edge are deployed in an active/standby configuration; if the primary appliance fails, then the secondary appliance will take over all firewall operations, and the IPS module in the secondary appliance inspects the traffic.

Figure 13 - IPS processing flowchart

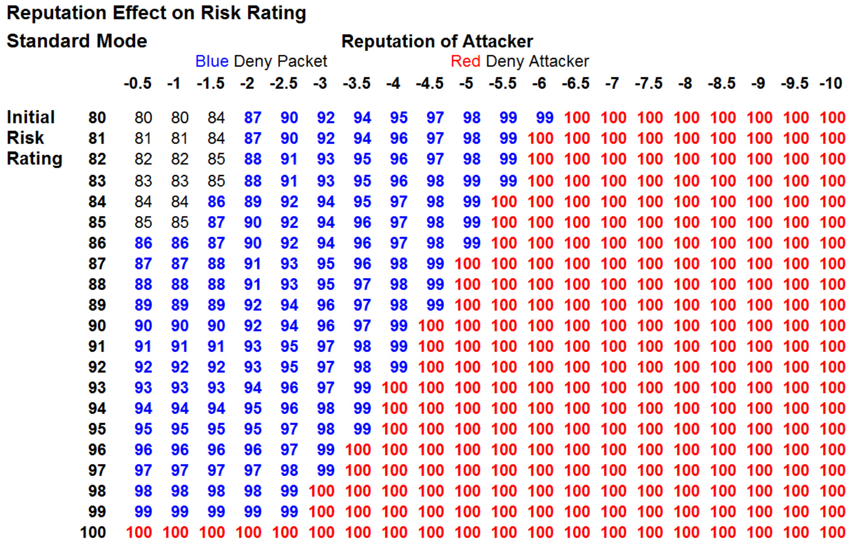


Cisco IPS can make informed decisions on whether to permit or block traffic based off of reputation. Cisco IPS uses reputation in two key ways:

- 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 addresses based off of prior behavior

Reputation Filters allow the IPS to block all traffic from known bad addresses before any significant inspection is done. Global Correlation Inspection uses the reputation of the attacker in conjunction with the risk rating associated with the signature in order to determine a new risk rating and drop traffic that is likely to be malicious.

Figure 14 - Reputation effect on risk rating



Reputation Effect on Risk Rating

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	100
	81	81	81	84	87	90	92	94	96	97	98	99	100	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	100
	83	83	83	85	88	91	93	95	96	98	99	99	100	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	100
	85	85	85	87	90	92	94	96	97	98	99	100	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	100
	87	87	87	88	91	93	95	96	98	99	100	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	100
	89	89	89	89	92	94	96	97	98	99	100	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	100
	91	91	91	91	93	95	97	98	99	100	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	100
	93	93	93	93	94	96	97	99	100	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	100
	95	95	95	95	95	97	98	99	100	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	100
	97	97	97	97	97	98	99	100	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	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	100	100

Reader Tip

For more information about how traffic moves through the Cisco ASA and AIP-SSM combination, see: http://www.cisco.com/en/US/docs/security/asa/asa84/asdm64/configuration_guide/modules_ips.html#wp1087140

Deployment Details

The first step used to configure an AIP-SSM is to session into the module from the appliance and set up basic networking such as IP address, gateway, and access lists in order 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 Cisco ASA Security Device Manager (ASDM) or the IPS Manager Express (IME).

Process

Configuring AIP-SSM

1. Complete the initial setup
2. Complete the startup wizard
3. Configure the policy
4. Modify the inline security policy
5. Configure the resilient AIP-SSM

Procedure 1 Complete the initial setup

Step 1: Configure the LAN distribution switch interfaces that are connected to the AIP-SSM management interface.

```
interface GigabitEthernet1/0/19
 description IE-SSM40a
!
interface GigabitEthernet2/0/19
 description IE-SSM40b
!
interface range GigabitEthernet1/0/19, GigabitEthernet2/0/19
 switchport access vlan 300
 switchport host
```

Step 2: From the Cisco ASA appliance, session into the module.

After logging into the appliance, 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. Enter the current password, and then input a new password. Change the password to a value that complies with the security policy of the organization.

```
login: cisco
Password:[password]
```

Step 3: Run the **setup** command.

```
sensor# setup
Enter host name[sensor]: IE-SSM40a
Enter IP interface[]: 10.4.24.27/27,10.4.24.1
Modify current access list?[no]: yes
Current access list entries:
   No entries
Permit: 0.0.0.0/0
Permit:
Use DNS server for Global Correlation?[no]: yes
   DNS server IP address[]: 10.4.48.10
Use HTTP proxy server for Global Correlation?[no]: no
Modify system clock settings?[no]: no
Participation in the SensorBase Network allows Cisco to
collect aggregated statistics about traffic sent to your IPS.
SensorBase Network Participation level?[off]: partial
Do you agree to participate in the SensorBase Network?[no]:yes

[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

Warning: The node must be rebooted for the changes to go into
effect.
Continue with reboot? [yes]:yes
```

You will now configure the second module.

Step 4: To return to the Cisco ASA command line, type **exit**.

Step 5: For the second AIP-SSM on the standby appliance, log in to the CLI, and repeat Step 3 to configure the basic network connectivity.

Tech Tip

A different host name and IP address must be used on the second AIP-SSM so that monitoring systems do not get confused. In this example, SSM-40-B and 10.4.24.28 was used on the standby SSM.

Procedure 2 Complete the startup wizard

You will now connect to the sensor in Cisco ASDM.

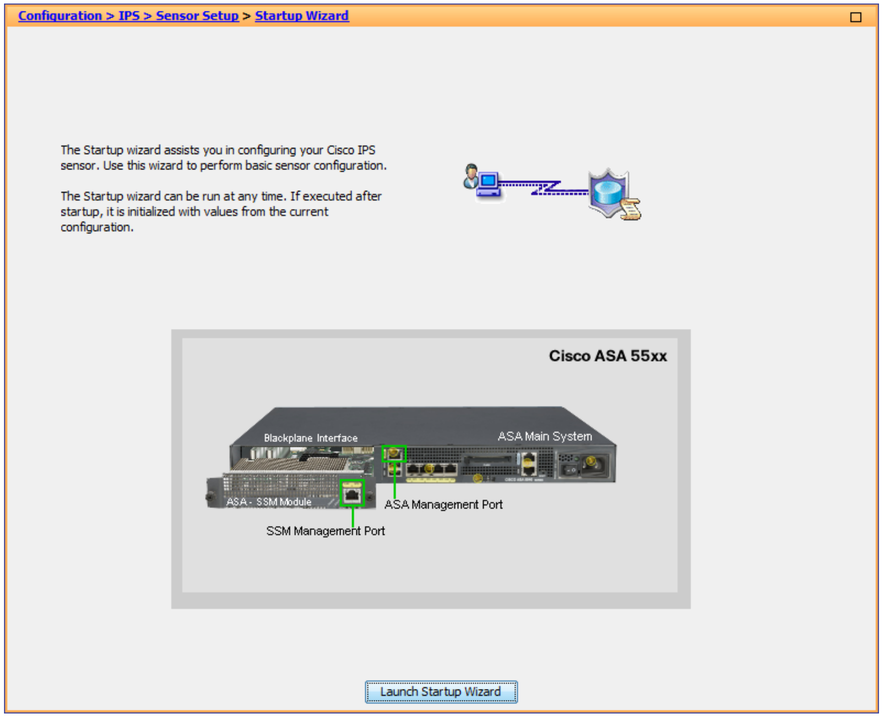
Step 1: From a client on the internal network, navigate to the firewall's inside IP address, and launch the Cisco ASA Security Device Manager. (Example: https://ie-asa5540.cisco.local/)

Step 2: Click on the **Configuration** tab, and then click **IPS**.

Step 3: In the **Connecting to IPS** dialog box, enter the username and password you specified on the IPS sensor, and then click **Continue.**

Cisco ASDM imports the current configuration from the IPS sensor, and the startup wizard launcher is displayed in the main window.

Step 4: Click **Launch Startup Wizard**.

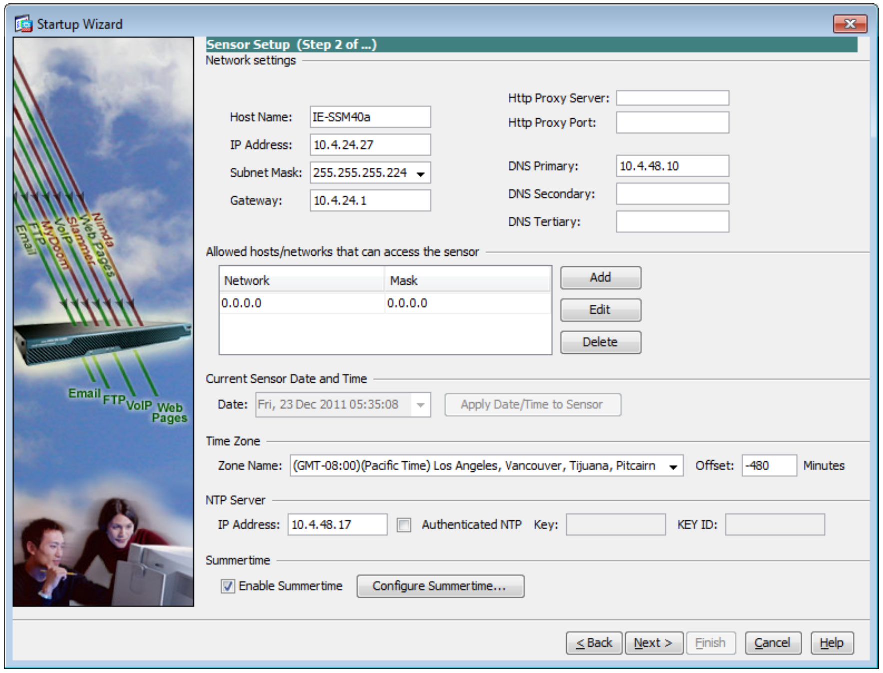


Configuration > IPS > Sensor Setup > Startup Wizard

The Startup wizard assists you in configuring your Cisco IPS sensor. Use this wizard to perform basic sensor configuration.

The Startup wizard can be run at any time. If executed after startup, it is initialized with values from the current configuration.

Step 5: 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 then click **Next.**



Startup Wizard

Sensor Setup (Step 2 of ...)

Network settings

Host Name: IE-SSM40a

IP Address: 10.4.24.27

Subnet Mask: 255.255.255.224

Gateway: 10.4.24.1

Http Proxy Server:

Http Proxy Port:

DNS Primary: 10.4.48.10

DNS Secondary:

DNS Tertiary:

Allowed hosts/networks that can access the sensor

Network	Mask
0.0.0.0	0.0.0.0

Current Sensor Date and Time

Date: Fri, 23 Dec 2011 05:35:08

Time Zone

Zone Name: (GMT-08:00)(Pacific Time) Los Angeles, Vancouver, Tijuana, Pitcairn Offset: -480 Minutes

NTP Server

IP Address: 10.4.48.17 □ Authenticated NTP Key: KEY ID:

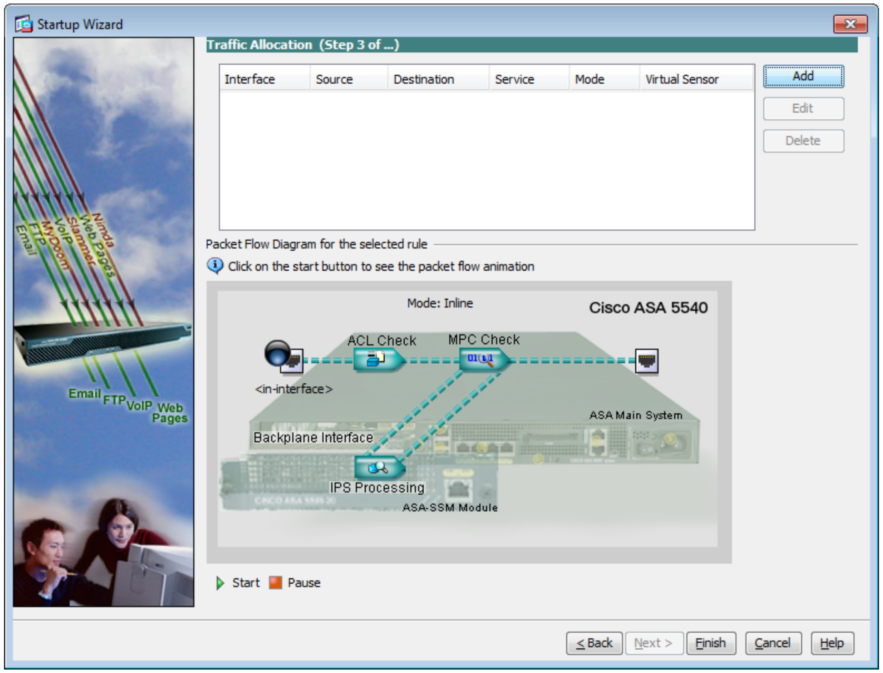
Summertime

☑ Enable Summertime

Procedure 3 Configure the policy

You must now decide the sensor mode. In IPS mode, the sensor is inline in the traffic path. In this mode, the sensor inspects and can drop traffic that is malicious. Alternatively, in IDS mode, a copy of the traffic is passively sent to the sensor. The sensor inspects, and can alerts on traffic that 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. You can deploy IDS mode 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.

Step 1: In **Startup Wizard: Traffic Allocation**, click **Add**.



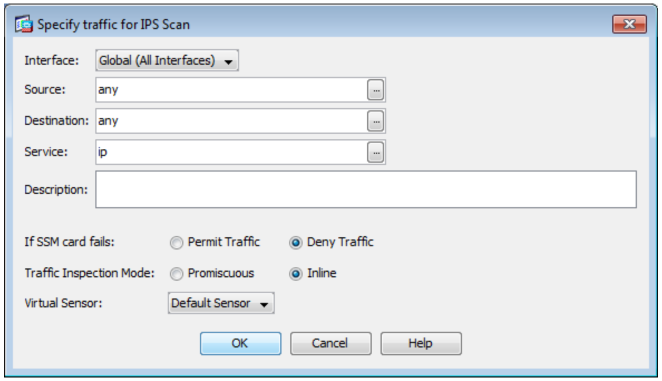
Interface	Source	Destination	Service	Mode	Virtual Sensor

Packet Flow Diagram for the selected rule

Click on the start button to see the packet flow animation

Step 2: If you are configuring an IPS policy, accept the default settings to inspect all traffic, and then then click **OK.**

If you are configuring an IDS policy, for **Traffic Inspection Mode**, select **Promiscuous**, and then click **OK**.



Interface: Global (All Interfaces)

Source: any

Destination: any

Service: ip

Description:

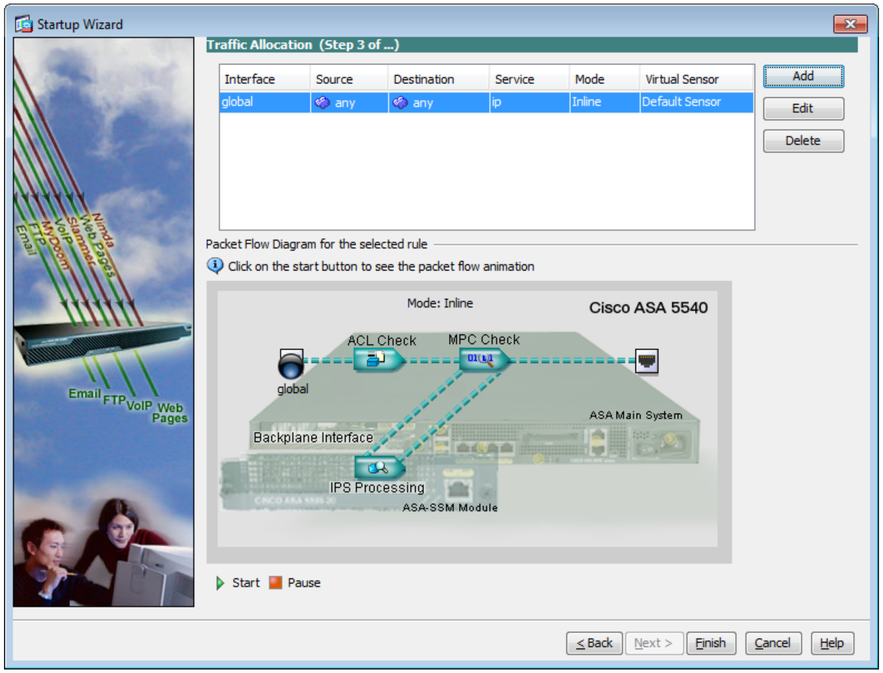
If SSM card fails: ○ Permit Traffic ● Deny Traffic

Traffic Inspection Mode: ○ Promiscuous ● Inline

Virtual Sensor: Default Sensor

Step 3: A global policy has been configured and is ready to be applied to the sensor. Click **Finish.**

Step 4: On the **Confirm Configuration Changes** dialog box, click **Yes.**

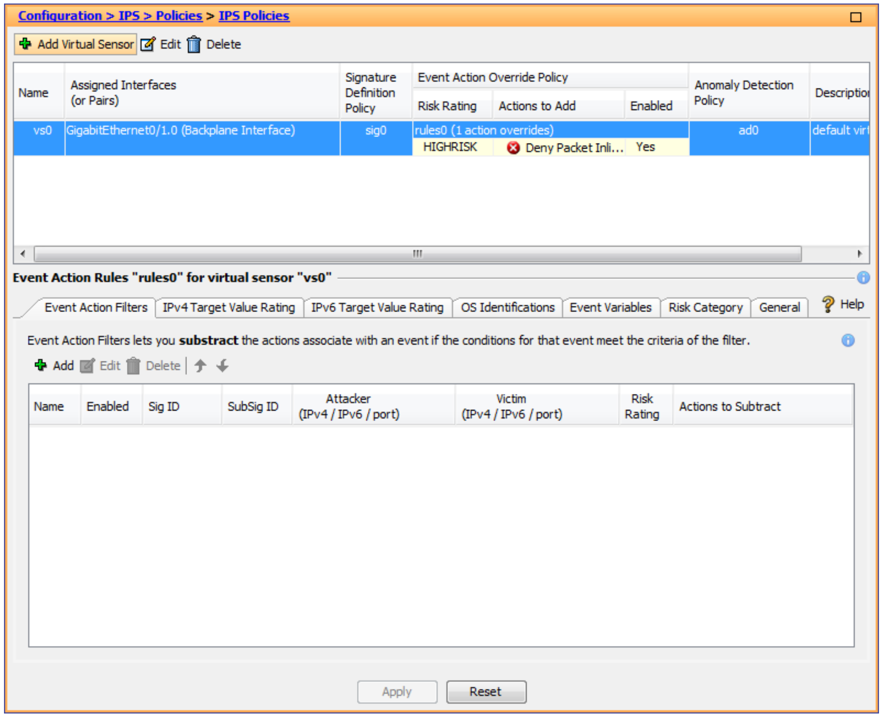


Interface	Source	Destination	Service	Mode	Virtual Sensor
global	any	any	ip	Inline	Default Sensor

Packet Flow Diagram for the selected rule

Click on the start button to see the packet flow animation

Step 5: To apply the policy to an interface, in the left hand window, click **Policies > IPS: Policies**, and then click **Edit**.



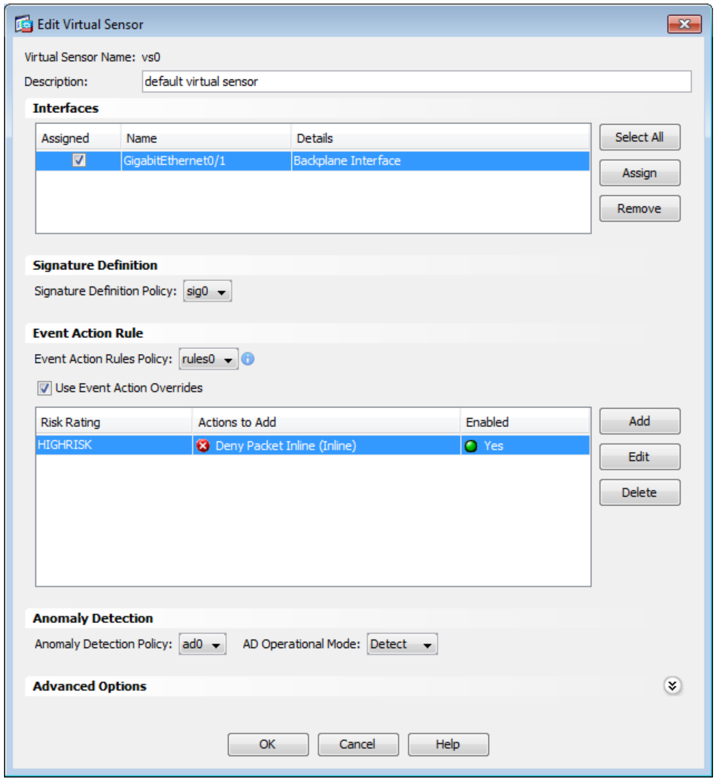
Name	Assigned Interfaces (or Pairs)	Signature Definition Policy	Event Action Override Policy			Anomaly Detection Policy	Descriptio
			Risk Rating	Actions to Add	Enabled		
vs0	GigabitEthernet0/1.0 (Backplane Interface)	sig0	rules0 (1 action overrides)			ad0	default vir
			HIGHRISK	Deny Packet Inli...	Yes		

Event Action Rules "rules0" for virtual sensor "vs0"

Event Action Filters lets you **substract** the actions associate with an event if the conditions for that event meet the criteria of the filter.

Name	Enabled	Sig ID	SubSig ID	Attacker (IPv4 / IPv6 / port)	Victim (IPv4 / IPv6 / port)	Risk Rating	Actions to Subtract

Step 6: In the **Edit Virtual Sensor** dialog box, select **Assigned**, click **Assign**, and then click **OK.**



Virtual Sensor Name: vs0

Description: default virtual sensor

Interfaces

Assigned	Name	Details
☑	GigabitEthernet0/1	Backplane Interface

Signature Definition

Signature Definition Policy: sig0

Event Action Rule

Event Action Rules Policy: rules0

☑ Use Event Action Overrides

Risk Rating	Actions to Add	Enabled
HIGHRISK	Deny Packet Inline (Inline)	Yes

Anomaly Detection

Anomaly Detection Policy: ad0 AD Operational Mode: Detect

Advanced Options

Step 7: To complete the setup, click **Apply** and save the appliance configuration.

If you configured an IPS policy, continue to the next procedure.

If you configured an IDS policy, skip the next procedure.

Procedure 4 Modify the inline security policy

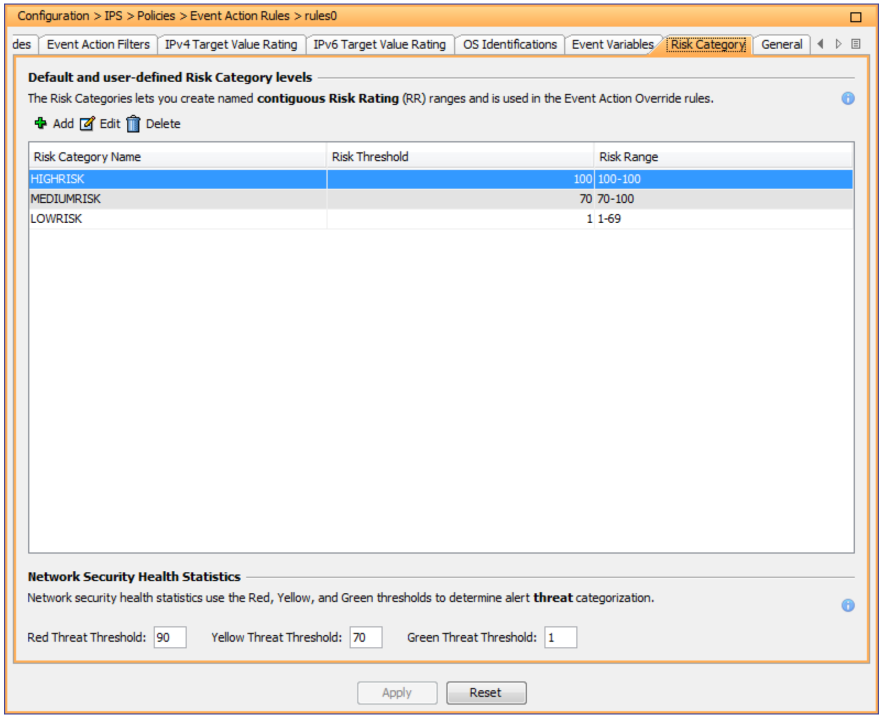
(Optional)

If you opted to run IPS mode, the sensor is configured to drop high-risk traffic. By default, this means that if an alert fires with a risk rating of at least 90 or if the traffic comes from an IP address with a negative reputation that raises the risk rating to 90 or higher, the sensor drops the traffic. If the risk rating is raised to 100 because of the source address reputation score, then the sensor drops all traffic from that IP address.

The chances of the IPS dropping traffic that is not malicious when using a risk threshold of 90 is very low. However, if you want to adopt a more conservative policy, for the risk threshold, raise the value to 100.

Step 1: Navigate to **Configuration > IPS > Policies > Event Action Rules > rules0**.

Step 2: In the **Risk Category** tab, select **HIGHRISK**, and then click **Edit**.



Default and user-defined Risk Category levels

The Risk Categories lets you create named **contiguous Risk Rating** (RR) ranges and is used in the Event Action Override rules.

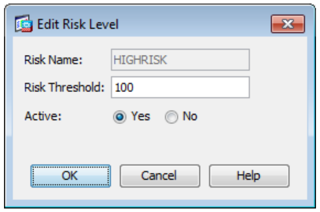
Risk Category Name	Risk Threshold	Risk Range
HIGHRISK	100	100-100
MEDIUMRISK	70	70-100
LOWRISK	1	1-69

Network Security Health Statistics

Network security health statistics use the Red, Yellow, and Green thresholds to determine alert **threat** categorization.

Red Threat Threshold: 90 Yellow Threat Threshold: 70 Green Threat Threshold: 1

Step 3: In the **Edit Risk Level** dialog box, in the **Risk Threshold box**, enter **100**, and then click **OK**.



Risk Name: HIGHRISK
Risk Threshold: 100
Active: ● Yes ○ No

Step 4: To complete the setup, click **Apply** and save the appliance configuration.

Procedure 5 Configure the resilient AIP-SSM

Step 1: From a client on the internal network, navigate to the standby firewall's inside IP address, and launch the Cisco ASA Security Device Manager. (Example: https://ie-asa5540-standby.cisco.local/)

Step 2: To configure the second IPS, repeat Procedure 2 - Procedure 4 using the name IE-SSM40a and the IP address 10.4.24.28/27.

Summary

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

Remote Access VPN

Business Overview

Many organizations need to offer network connectivity to their data resources for users, regardless of the user's 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
- Seamless access to networked data resources
- Authentication and policy control that integrates with the authentication resources in use by the organization
- Cryptographic security to prevent the exposure of sensitive data to unauthorized parties who accidentally or intentionally intercept the data

Technology Overview

The Cisco ASA family supports IPsec, web portal, full tunnel SSL VPNs for client-based remote access, and IPsec for site-to-site VPN. This section describes the basic configuration of SSL VPNs for remote access.

The Cisco AnyConnect Secure Mobility Client is recommended for remote users who require full network connectivity. 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 companies block HTTPS access out of their networks.

The Cisco Smart Business Architecture Borderless Network for Enterprise 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 number 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 Cisco AnyConnect for SSL connections. The configuration is broken into sections for each of the various access methods, and it 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 the 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.

Table 5 - Hardware performance

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

A different VPN group is required for each remote-access policy. This design includes three VPN groups:

- **Administrative users**—are authenticated by Cisco Secure Access Control Server (ACS) using the RADIUS protocol and also have a local username and password fallback option. This ensures that VPN access is available when the Cisco Secure ACS or Microsoft Active Directory server is unavailable. Administrative users have full access to the entire network.
- **Employees**—are authenticated by Cisco Secure ACS and have open access to the entire network
- **Partners**—are authenticated by Cisco Secure ACS and, although they use a tunnel-all VPN policy, there is an access-list applied to the tunnels in order to restrict access to specific hosts.

Deployment Details

Reader Tip

For more information about the baseline configuration of the appliance (including availability, routing, Internet and inside connectivity, and management/administration access), see the *Firewall* section of this guide.

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.

Process

Configuring Cisco Secure ACS

1. Define external groups
2. Create the device type group
3. Create the network device
4. Create authorization profiles
5. Configure the access service
6. Create authorization rules

Authentication is the portion of the configuration that verifies that users' credentials (username and password) match those stored within the organization's database of users that are allowed to access electronic resources. Cisco SBA Borderless Network for Enterprise uses Cisco Secure ACS for its authentication. When the Cisco ASA firewall queries the Cisco Secure ACS server (which then proxies the request to the Active Directory database) to determine whether a user's name and password is valid, Cisco Secure ACS also retrieves other Active Directory attributes that Cisco Secure ACS may use when making an authorization decision, such as group membership. Based on the group membership, Cisco Secure ACS sends back a group policy name to the appliance, along with the success or failure of the login. Cisco ASA uses the group policy name to assign the user to the appropriate VPN group policy.

In this process, Active Directory is the primary directory container for user credentials and group membership. Before you begin this process your Active Directory must have three groups, **vpn-administrator**, **vpn-employee**, and **vpn-partner,** defined that map users to the respective VPN access policies.

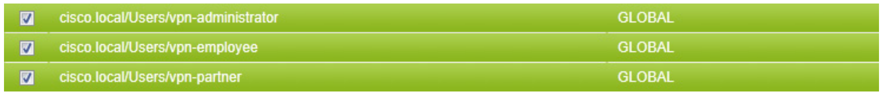
Procedure 1 Define external groups

Step 1: Navigate to the ACS Administration Page. (Example: https://acs.cisco.local)

Step 2: In **Users and Identity Stores > External Identity Stores > Active Directory**, click the **Directory Groups** tab.

Step 3: Click **Select**.

Step 4: On the **External User Groups** pane, select the three Active Directory groups, and then click **OK**.



☑	cisco.local/Users/vpn-administrator	GLOBAL
☑	cisco.local/Users/vpn-employee	GLOBAL
☑	cisco.local/Users/vpn-partner	GLOBAL

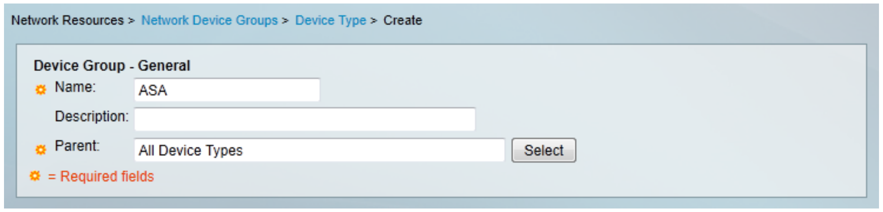
Step 5: On the Active Directory pane, click **Save Changes**.

Procedure 2 Create the device type group

Step 1: In **Network Resources > Network Device Groups > Device Type**, click **Create**.

Step 2: In the **Name** box, enter a name for the group. (Example: ASA)

Step 3: In the **Parent** box, select **All Device Types**, and then click **Submit**.



Network Resources > Network Device Groups > Device Type > Create

Device Group - General

- * Name: ASA
- Description:
- * Parent: All Device Types

* = Required fields

Procedure 3 Create the network device

For the Cisco ASA firewall, create a network device entry in the ACS.

Step 1: In **Network Resources > Network Devices and AAA Clients**, click **Create**.

Step 2: In the **Name** box, enter the device hostname. (Example: IE-ASA5540)

Step 3: In the **Device Type** box, select **All Device Types:ASA**.

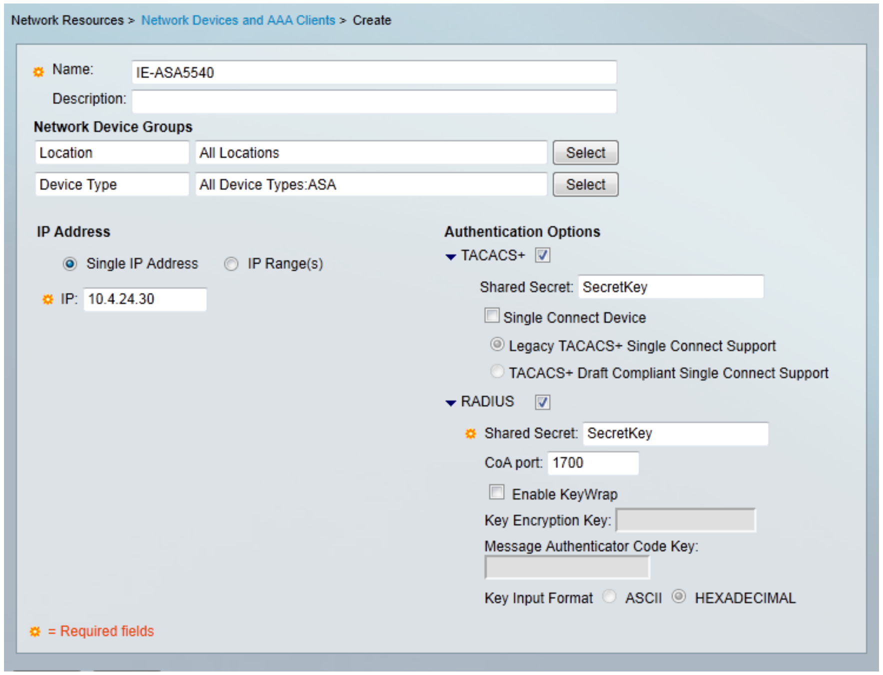
Step 4: In the **IP** box, enter the Cisco ASAs inside interface IP address. (Example: 10.4.24.30)

Step 5: Select **TACACS+**.

Step 6: Enter the TACACS+ shared secret key. (Example: SecretKey)

Step 7: Select **RADIUS**.

Step 8: Enter the RADIUS shared secret key, and then click **Submit**. (Example SecretKey)



Network Resources > Network Devices and AAA Clients > Create

- * Name: IE-ASA5540
- Description:

Network Device Groups

Location	All Locations	Select
Device Type	All Device Types:ASA	Select

IP Address

● Single IP Address ○ IP Range(s)

* IP: 10.4.24.30

Authentication Options

▾ TACACS+ ☑

Shared Secret: SecretKey

□ Single Connect Device

● Legacy TACACS+ Single Connect Support

○ TACACS+ Draft Compliant Single Connect Support

▾ RADIUS ☑

* Shared Secret: SecretKey

CoA port: 1700

□ Enable KeyWrap

Key Encryption Key:

Message Authenticator Code Key:

Key Input Format ○ ASCII ● HEXADECIMAL

* = Required fields

Procedure 4 Create authorization profiles

Create two different authorization profiles to identify users that belong to either vpn-administrator or vpn-partner in Active Directory.

Step 1: In **Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles**, click **Create.**

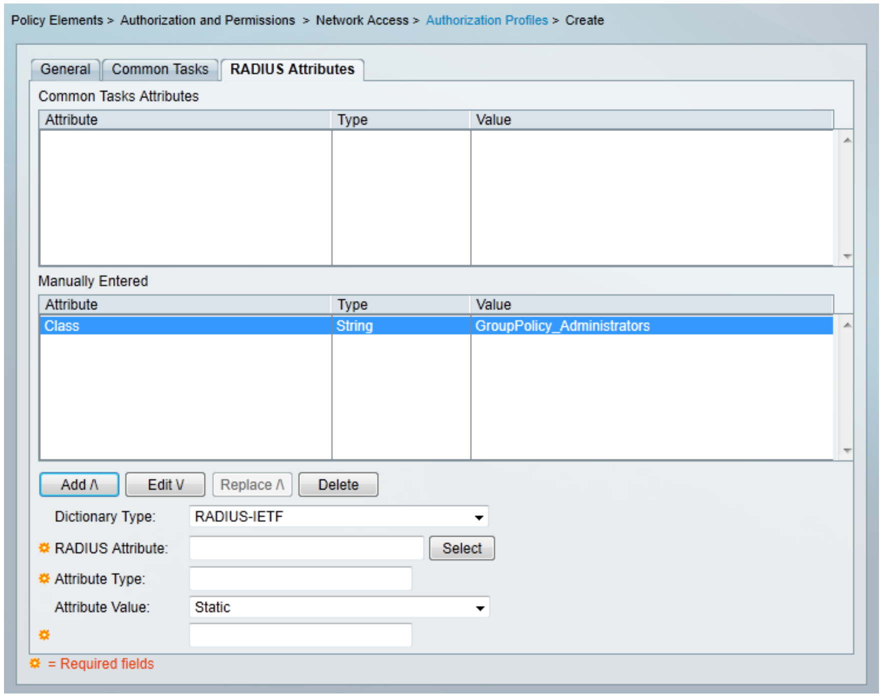
Step 2: In the **Name** box, enter a name for the authorization profile. (Example: RA-Administrator)

Step 3: Select the **RADIUS Attributes** tab.

Step 4: In the **RADIUS Attribute** box, select **Class**.

Next, you must configure the attribute value to match the group policy that you will configure on the Cisco ASA.

Step 5: In the **Value** box enter the group policy name, and then click **Add**. (Example: GroupPolicy_Administrators)



Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Create

Common Tasks Attributes

Attribute	Type	Value

Manually Entered

Attribute	Type	Value
Class	String	GroupPolicy_Administrators

Dictionary Type: RADIUS-IETF

RADIUS Attribute:

Attribute Type:

Attribute Value: Static

= Required fields

Step 6: Repeat the procedure to build an authorization profile for partners, using the group policy **GroupPolicy_Partner** value.

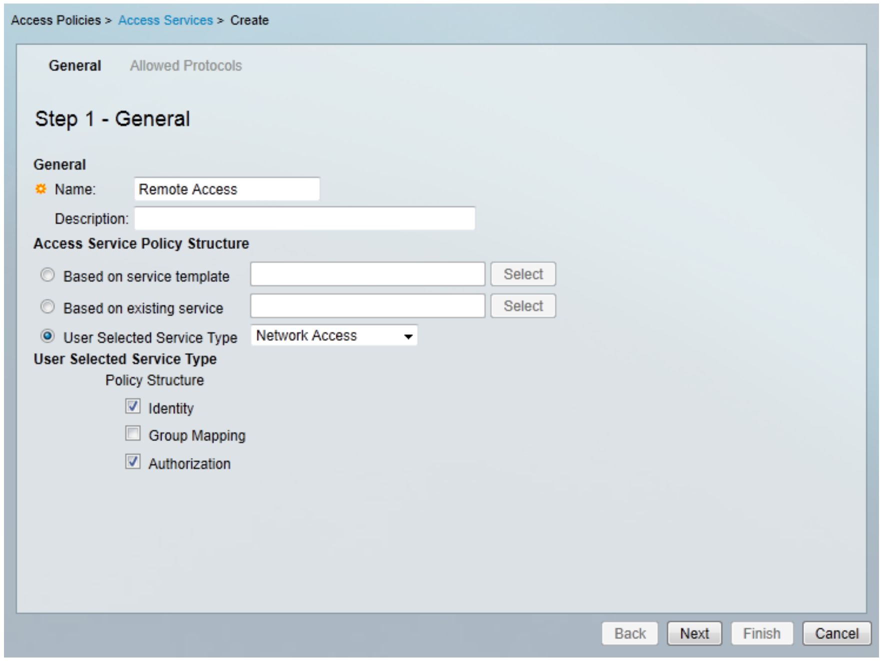
Procedure 5 Configure the access service

Create a policy to inspect the return traffic from the Active Directory server for group membership.

Step 1: In **Access Policies > Access Services** click **Create**.

Step 2: On the **General** tab, enter the name **Remote Access**.

Step 3: Select **User Selected Service Type** and then click **Next**.



Access Policies > Access Services > Create

Step 1 - General

General

Name: Remote Access

Description:

Access Service Policy Structure

○ Based on service template

○ Based on existing service

● User Selected Service Type Network Access

User Selected Service Type

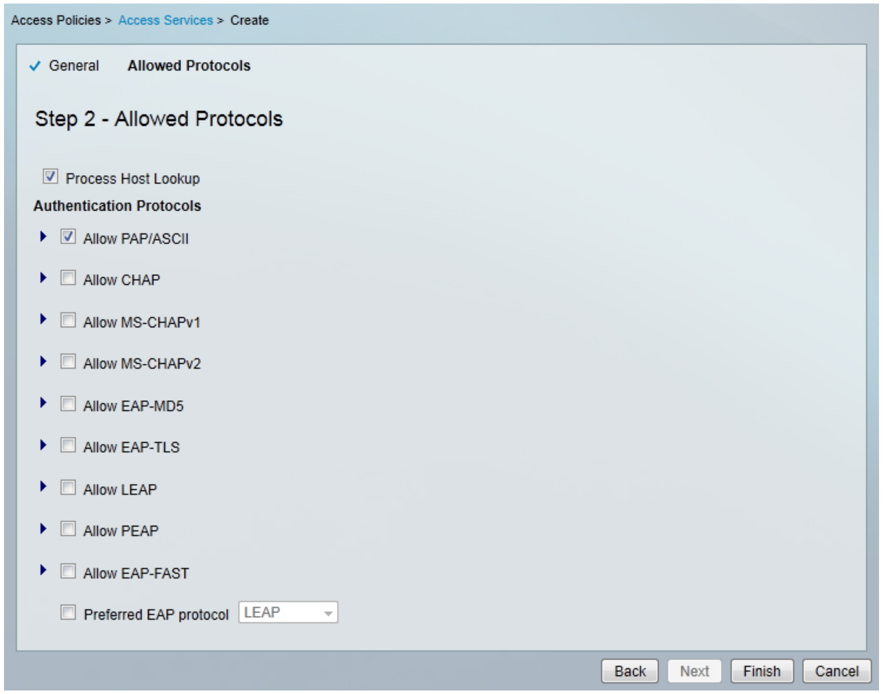
Policy Structure

☑ Identity

☐ Group Mapping

☑ Authorization

Step 4: On the **Allowed Protocols** tab, select **Allow PAP/ASCII, and then click Finish.**



Access Policies > Access Services > Create

✓ General Allowed Protocols

Step 2 - Allowed Protocols

☑ Process Host Lookup

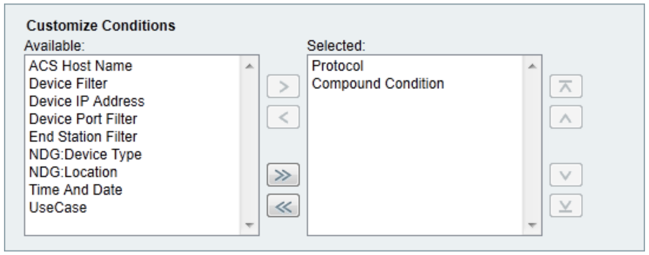
Authentication Protocols

- ☑ Allow PAP/ASCII
- □ Allow CHAP
- □ Allow MS-CHAPv1
- □ Allow MS-CHAPv2
- □ Allow EAP-MD5
- □ Allow EAP-TLS
- □ Allow LEAP
- □ Allow PEAP
- □ Allow EAP-FAST

□ Preferred EAP protocol: LEAP

Step 5: In **Access Policies > Access Services > Service Selection Rules,** click **Customize**.

Step 6: On the Customize Conditions pane, move **Compound Condition** from **Available** to **Selected**, and then click **OK**.



Customize Conditions

Available:
ACS Host Name
Device Filter
Device IP Address
Device Port Filter
End Station Filter
NDG:Device Type
NDG:Location
Time And Date
UseCase

Selected:
Protocol
Compound Condition

Step 7: On the **Service Selection Rules** pane, click **Create**.

Step 8: In the browser, name the rule **Remote Access**.

Step 9: Select **Protocol.**

Step 10: In the list at right, select **match**, and then in the box, enter **Radius**.

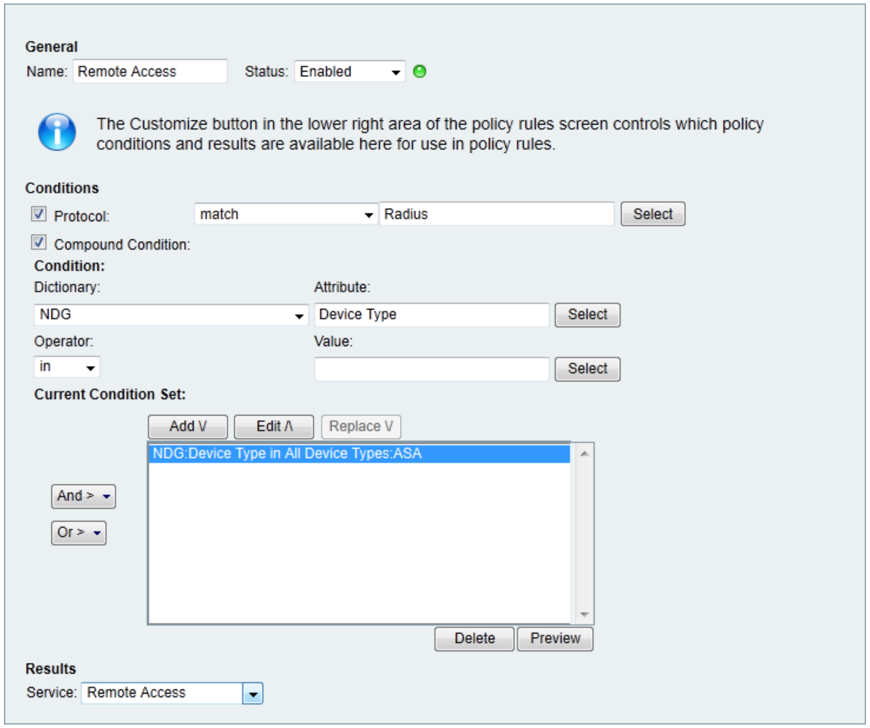
Step 11: Select **Compound Condition**, and then in the **Dictionary** list, choose **NDG**.

Step 12: For **Attribute**, select **Device Type.**

Step 13: For **Value**, select **All Device Types:ASA**.

Step 14: Under **Current Condition Set**, click **Add V**. The information is added to the Current Condition Set.

Step 15: In the **Results Service** list, choose **Remote Access, and then click OK.**



General

Name: Remote Access Status: Enabled

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions

☑ Protocol: match Radius

☑ Compound Condition:

Condition:

Dictionary: NDG

Attribute: Device Type

Operator: in

Value:

Current Condition Set:

NDG:Device Type in All Device Types:ASA

Results

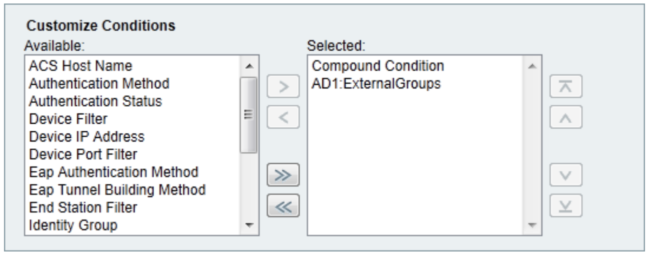
Service: Remote Access

Step 16: Navigate to **Access Policies > Access Services > Remote Access > Identity.**

Step 17: In the **Identity Source** box, select **AD1**, and then click **Save Changes**.

Step 18: In **Access Policies > Access Services > Remote Access > Authorization,** click **Customize**.

Step 19: On the Customize Conditions pane, move **AD1:ExternalGroups** from **Available** to **Selected**, and then click **OK**.



Customize Conditions

Available:
- ACS Host Name
- Authentication Method
- Authentication Status
- Device Filter
- Device IP Address
- Device Port Filter
- Eap Authentication Method
- Eap Tunnel Building Method
- End Station Filter
- Identity Group

Selected:
- Compound Condition
- AD1:ExternalGroups

Procedure 6 Create authorization rules

Step 1: In **Access Policies > Access Services > Remote Access > Authorization,** click **Create**.

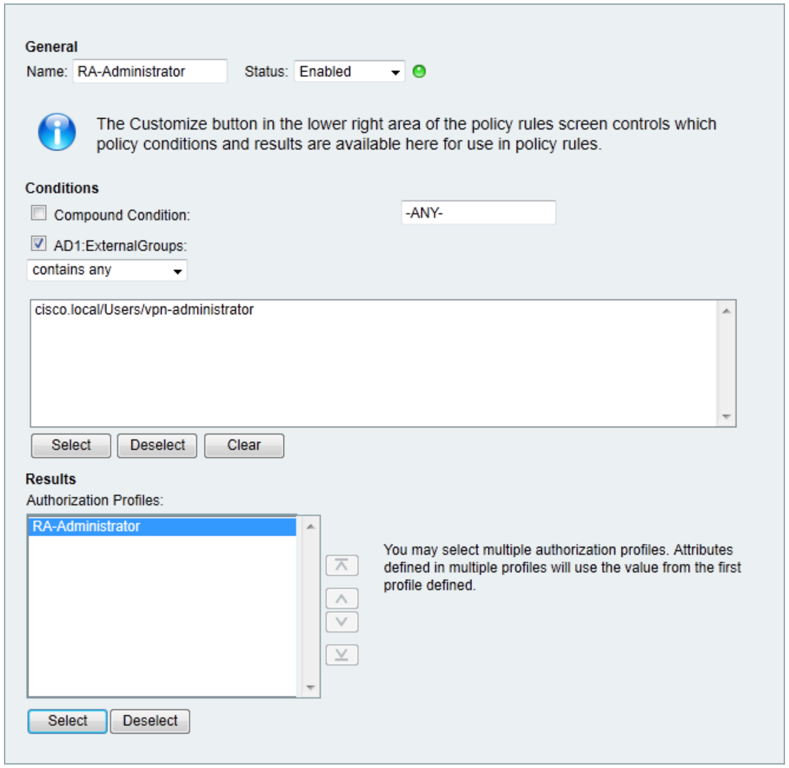
Step 2: Enter a rule **Name**.(Example: RA-Administrator)

Step 3: Under **Conditions**, select **AD1:ExternalGroups**.

Step 4: In the condition definition box, select the Active Directory group. (Example: cisco.local/Users/vpn-administrator).

Step 5: Under **Results**, select the authorization profile, and then click **OK**.

(Example: RA-Administrator)



General

Name: RA-Administrator Status: Enabled

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions

□ Compound Condition: -ANY-

☑ AD1:ExternalGroups:

contains any

cisco.local/Users/vpn-administrator

Results

Authorization Profiles:

RA-Administrator

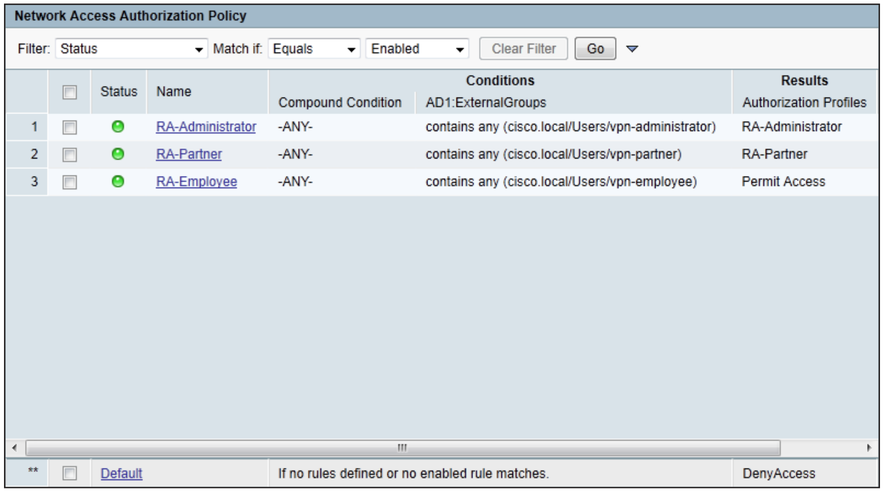
You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.

Step 6: Repeat the procedure for the partner rule.

Step 7: Repeat the procedure for the employee rule, using **Permit Access** as the authorization profile.

Step 8: On the Authorization pane, click the **Default** rule.

Step 9: Select **DenyAccess** as the authorization profile, and then click **OK.**



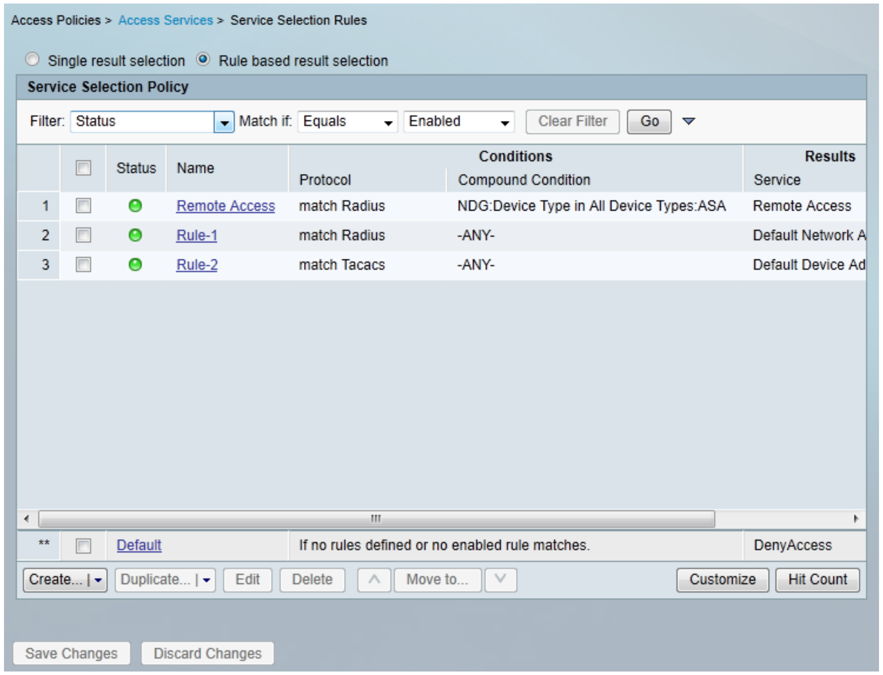
Network Access Authorization Policy

Filter: Status Match if: Equals Enabled

	□	Status	Name	Conditions		Results
				Compound Condition	AD1:ExternalGroups	Authorization Profiles
1	□	●	RA-Administrator	-ANY-	contains any (cisco.local/Users/vpn-administrator)	RA-Administrator
2	□	●	RA-Partner	-ANY-	contains any (cisco.local/Users/vpn-partner)	RA-Partner
3	□	●	RA-Employee	-ANY-	contains any (cisco.local/Users/vpn-employee)	Permit Access
**	□		Default	If no rules defined or no enabled rule matches.		DenyAccess

Once the remote-access services have been created, you can change the order.

Step 10: In **Access Policies > Access Services > Service Selection Rule s,** select the **Remote Access** policy, and then use the up arrows to move it to the first position.



Access Policies > Access Services > Service Selection Rules

○ Single result selection ● Rule based result selection

Service Selection Policy

Filter: Status Match if: Equals Enabled

	□	Status	Name	Conditions		Results
				Protocol	Compound Condition	Service
1	□	●	Remote Access	match Radius	NDG:Device Type in All Device Types:ASA	Remote Access
2	□	●	Rule-1	match Radius	-ANY-	Default Network A
3	□	●	Rule-2	match Tacacs	-ANY-	Default Device Ad
**	□		Default	If no rules defined or no enabled rule matches.		DenyAccess

Process

Configuring the Remote Access VPN

1. Configure remote access
2. Configure routing
3. Configure the group-URL
4. Configure resilient Internet connection
5. Configure the partner policy
6. Configure the admin policy
7. Cisco AnyConnect Client Profile

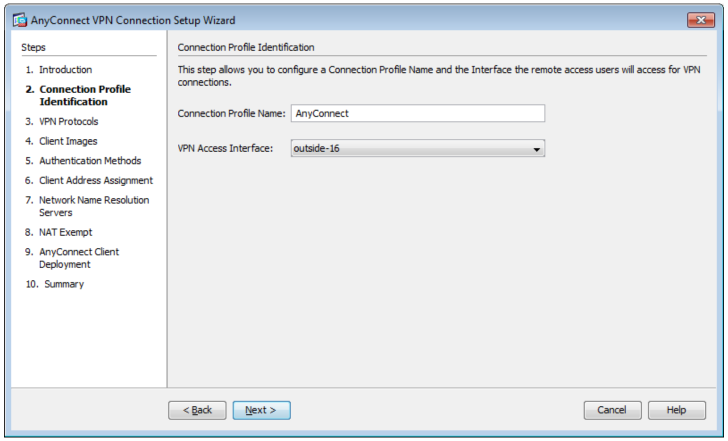
Procedure 1 Configure remote access

Step 1: Navigate to **Wizards > VPN Wizards > AnyConnect VPN Wizard...**

Step 2: In the **AnyConnect VPN Connection Setup Wizard** dialog box, click **Next**.

Step 3: Enter a **Connection Profile Name**. (Example: AnyConnect)

Step 4: In the **VPN Access Interface** list, select the primary Internet connection, and then click **Next**. (Example: outside-16)



AnyConnect VPN Connection Setup Wizard

Steps

1. Introduction
2. **Connection Profile Identification**
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. Client Address Assignment
7. Network Name Resolution Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary

Connection Profile Identification

This step allows you to configure a Connection Profile Name and the Interface the remote access users will access for VPN connections.

Connection Profile Name: AnyConnect

VPN Access Interface: outside-16

Generate a self-signed identity certificate and install it on the appliance.

Tech Tip

Note that because the certificate in this example is self-signed, clients will generate a security warning until they accept the certificate.

Step 5: In the **Digital Certificate** pane, click **Manage...**

Step 6: In the **Manage Identity Certificates** dialog box, click **Add**.

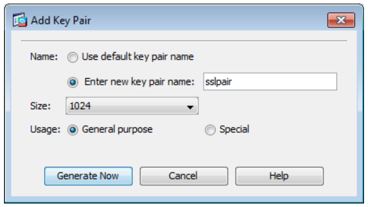
Step 7: On the **Add Identity Certificate** dialog box, select **Add a new identity certificate**.

Entering a new key pair name prevents the certificate from becoming invalid if an administrator accidentally regenerates the default RSA key pair.

Step 8: For **Key Pair**, select **New**.

Step 9: In the **Add Key Pair** dialog box, select **Enter new key pair name**, and then in the box, enter a name. (Example: sslpair)

Step 10: Click **Generate Now**.



Add Key Pair

Name: ○ Use default key pair name

● Enter new key pair name: sslpair

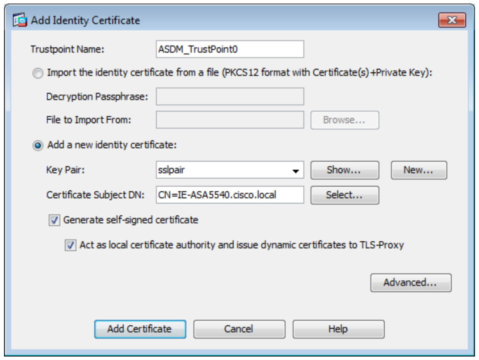
Size: 1024

Usage: ● General purpose ○ Special

Step 11: In the **Add Identity Certificate** dialog box, in **Certificate Subject DN**, enter the fully qualified domain name used to access the appliance on the outside interface. (Example: CN=IE-ASA5540.cisco.local)

Step 12: Select **Generate self-signed certificate** and **Act as Local certificate authority and issue dynamic certificates to TLS-Proxy.**

Step 13: Click **Add Certificate.**



Add Identity Certificate

Trustpoint Name: ASDM_TrustPoint0

○ Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

● Add a new identity certificate:

Key Pair: sslpair

Certificate Subject DN: CN=IE-ASA5540.cisco.local

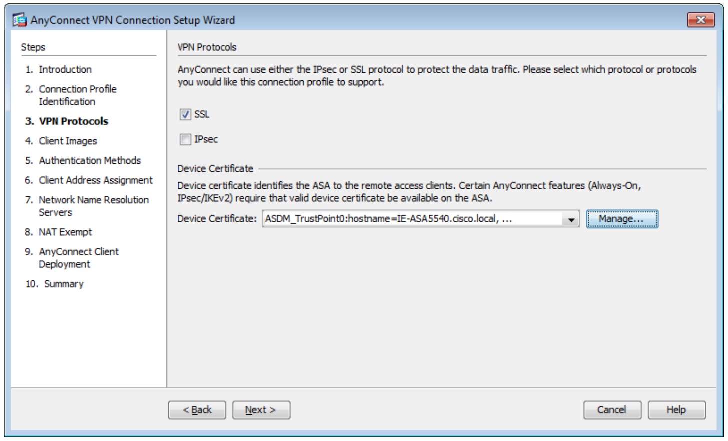
☑ Generate self-signed certificate

☑ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

Step 14: The **Enrollment Status** dialog box shows that the enrollment succeeded. Click **OK**.

Step 15: In the **Manage Identity Certificates** dialog box, click **OK**.

Step 16: On the **VPN Protocols** page, clear **IPsec**, and then click **Next**.



AnyConnect VPN Connection Setup Wizard

VPN Protocols

AnyConnect can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol or protocols you would like this connection profile to support.

☑ SSL

□ IPsec

Device Certificate

Device certificate identifies the ASA to the remote access clients. Certain AnyConnect features (Always-On, IPsec/IKEv2) require that valid device certificate be available on the ASA.

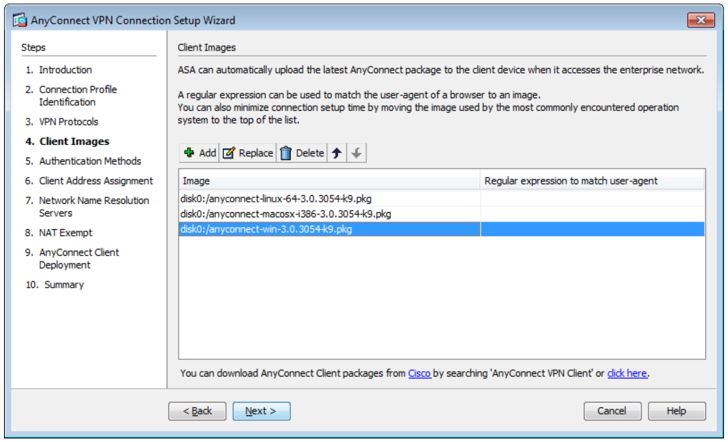
Device Certificate: ASDM_TrustPoint0:hostname=IE-ASA5540.cisco.local, ...

Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. Client Address Assignment
7. Network Name Resolution Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary
Manage...
< Back
Next >
Cancel
Help

Step 17: Click **Add**, select the Cisco AnyConnect client image that matches the remote user's platform, and then click **OK**.

Step 18: Repeat the previous step for all the required Cisco AnyConnect client images.

Step 19: On the **Client Images** page, click **Next**.



AnyConnect VPN Connection Setup Wizard

Client Images

ASA can automatically upload the latest AnyConnect package to the client device when it accesses the enterprise network.

A regular expression can be used to match the user-agent of a browser to an image.
You can also minimize connection setup time by moving the image used by the most commonly encountered operation system to the top of the list.

Image	Regular expression to match user-agent
disk0:/anyconnect-linux-64-3.0.3054-k9.pkg	
disk0:/anyconnect-macosx-i386-3.0.3054-k9.pkg	
disk0:/anyconnect-win-3.0.3054-k9.pkg	

You can download AnyConnect Client packages from Cisco by searching 'AnyConnect VPN Client' or click here.

Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. Client Address Assignment
7. Network Name Resolution Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary
Add
Replace
Delete
< Back
Next >
Cancel
Help

Next, you will create a new AAA server group that uses RADIUS to authenticate remote-access users.

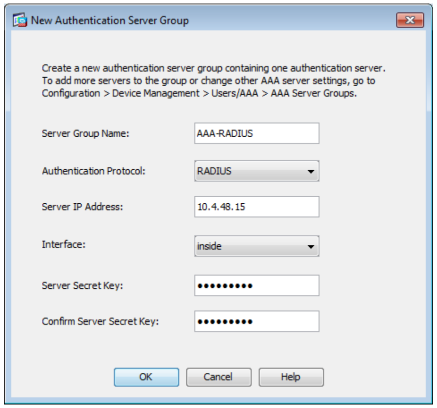
Step 20: On the **Authentication Methods** pane, click **New**.

Step 21: In the **New Authentication Server Group** dialog box, enter a **Server Group Name**. (Example: AAA-RADIUS)

Step 22: In the **Server IP Address** box, enter the IP address of the Cisco Secure ACS server. (Example: 10.4.48.15)

Step 23: In the **Interface** list, select **inside**.

Step 24: Enter and confirm the **Secret Key**, and then click **OK**. (Example: SecretKey)



Create a new authentication server group containing one authentication server. To add more servers to the group or change other AAA server settings, go to Configuration > Device Management > Users/AAA > AAA Server Groups.

Server Group Name: AAA-RADIUS

Authentication Protocol: RADIUS

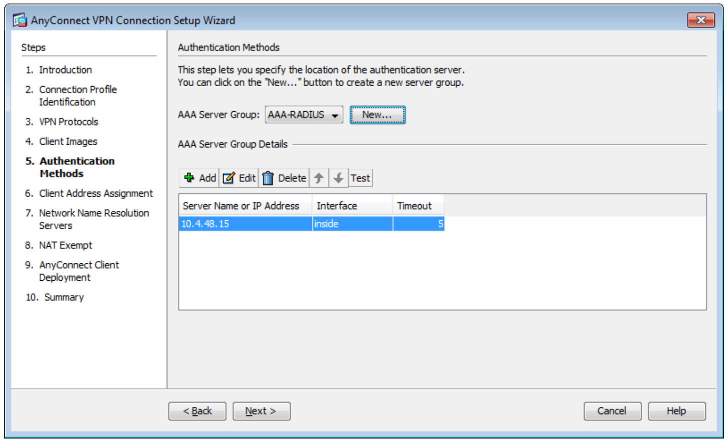
Server IP Address: 10.4.48.15

Interface: inside

Server Secret Key: ••••••••••

Confirm Server Secret Key: ••••••••••

Step 25: On the **Authentication Methods** page, click **Next**.


AnyConnect VPN Connection Setup Wizard
Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. Client Address Assignment
7. Network Name Resolution Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary
New...
Add
Edit
Delete
Test
< Back
Next >
Cancel
Help

Authentication Methods

This step lets you specify the location of the authentication server. You can click on the "New..." button to create a new server group.

AAA Server Group: AAA-RADIUS

AAA Server Group Details

Server Name or IP Address	Interface	Timeout
10.4.48.15	inside	5

Next, you will define the remote-access VPN address pool that will be assigned to users when they connect to the VPN service.

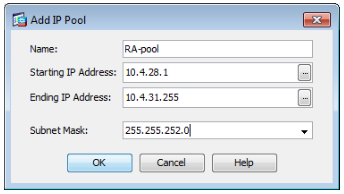
Step 26: On the **IPv4 Address Pool** tab, click **New**.

Step 27: On the **Add IP Pool** dialog box, enter a **Name**. (Example: RA-pool)

Step 28: Enter the **Starting IP Address** for the pool. (Example: 10.4.28.1)

Step 29: Enter the **Ending IP Address** for the pool. (Example: 10.4.31.255)

Step 30: Enter the pool's **Subnet Mask**, and then click **OK**. (Example: 255.255.252.0)



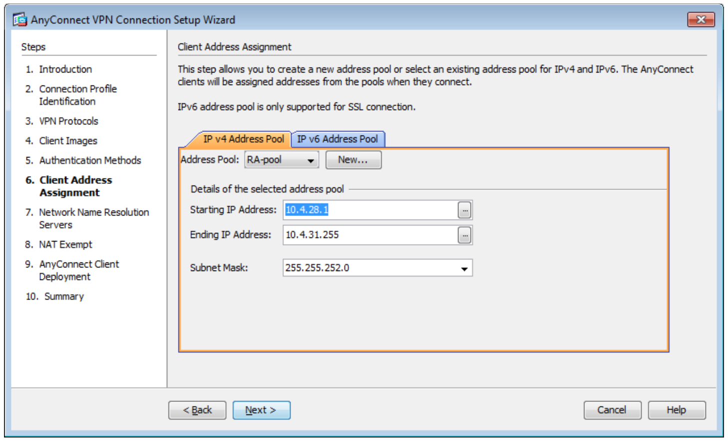
Name: RA-pool

Starting IP Address: 10.4.28.1

Ending IP Address: 10.4.31.255

Subnet Mask: 255.255.252.0

Step 31: On the **Client Address Assignment** page, click **Next**.


AnyConnect VPN Connection Setup Wizard
Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. Client Address Assignment
7. Network Name Resolution Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary
IP v4 Address Pool
IP v6 Address Pool
New...
< Back
Next >
Cancel
Help

Client Address Assignment

This step allows you to create a new address pool or select an existing address pool for IPv4 and IPv6. The AnyConnect clients will be assigned addresses from the pools when they connect.

IPv6 address pool is only supported for SSL connection.

Address Pool: RA-pool

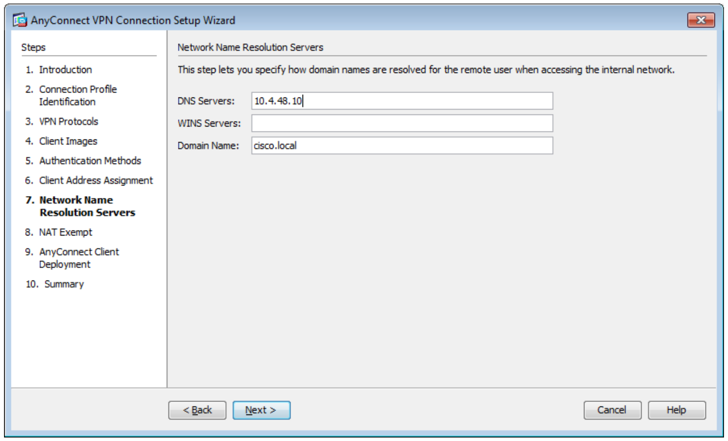
Details of the selected address pool

Starting IP Address: 10.4.28.1

Ending IP Address: 10.4.31.255

Subnet Mask: 255.255.252.0

Step 32: In the wizard, on the **Network Name Resolution Servers** page, enter the organization's **DNS Servers** (Example: 10.4.48.10) and the organization's **Domain Name**, and then click **Next**. (Example: cisco.local)


AnyConnect VPN Connection Setup Wizard

Network Name Resolution Servers

This step lets you specify how domain names are resolved for the remote user when accessing the internal network.

DNS Servers: 10.4.48.10

WINS Servers:

Domain Name: cisco.local

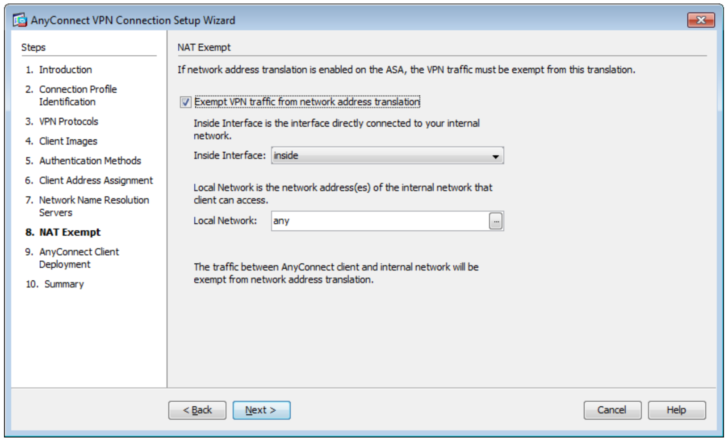
Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. Client Address Assignment
7. Network Name Resolution Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary
< Back
Next >
Cancel
Help

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 be translated, which would change the source address of the traffic, making it impossible for clients to receive traffic correctly from servers with which they communicate.

Step 33: If you are implementing a 10K design, skip to Step 36. If you are implementing a 5K design, in the wizard, on the **NAT Exempt** page, select **Exempt traffic from network address translation**.

Step 34: In the **Inside Interface** list, select **inside**.

Step 35: In the **Local Network** box, enter **any**, and then click **Next**.


AnyConnect VPN Connection Setup Wizard

NAT Exempt

If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation.

☑ Exempt VPN traffic from network address translation

Inside Interface is the interface directly connected to your internal network.

Inside Interface: inside

Local Network is the network address(es) of the internal network that client can access.

Local Network: any

The traffic between AnyConnect client and internal network will be exempt from network address translation.

Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. Client Address Assignment
7. Network Name Resolution Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary
< Back
Next >
Cancel
Help

Step 36: On the **AnyConnect Client Deployment** page, click **Next**, and then on the **Summary** page, click **Finish**.

Finally, you must upload the Cisco AnyConnect client images to the secondary appliance.

Step 37: On the secondary appliance, copy the Cisco AnyConnect client images to the local flash disk.

```
ftp://10.4.48.27/anyconnect-win-3.0.3054-k9 disk0:
ftp://10.4.48.27/anyconnect-macosx-i386-3.0.3054-k9 disk0:
ftp://10.4.48.27/anyconnect-linux-64-3.0.3054-k9 disk0:
```

Procedure 2 Configure routing

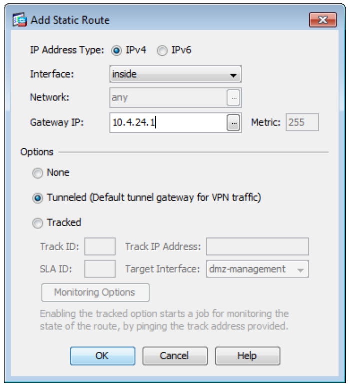
Traffic from remote-access VPN clients to and from the Internet must be inspected by the organization's firewall, IDS, and policy controls such as Cisco IronPort® Web Security Appliance. To accomplish this, all traffic to and from the VPN clients must be routed toward the LAN distribution switch, regardless of the traffic's destination, so that the Cisco ASA policy engine has the visibility to handle the traffic correctly.

Step 1: In **Configuration > Device Setup > Routing > Static Routes**, click **Add**.

Step 2: In the **Add Static Route** dialog box, in the **Interface** list, select **inside**.

Step 3: Select **Tunneled (Default tunnel gateway for VPN traffic)**.

Step 4: In the **Gateway IP** box, enter the Internet Edge VLAN interface IP address on the LAN distribution switch and then click **OK**. (Example: 10.4.24.1)



Add Static Route

IP Address Type: ● IPv4 ○ IPv6

Interface: inside

Network: any

Gateway IP: 10.4.24.1 Metric: 255

Options

○ None

● Tunneled (Default tunnel gateway for VPN traffic)

○ Tracked

Track ID: Track IP Address:

SLA ID: Target Interface: dmz-management

Monitoring Options

Enabling the tracked option starts a job for monitoring the state of the route, by pinging the track address provided.

Cisco ASA advertises the each connected user to the rest of the network as individual host routes. Summarizing the address-pool reduces the IP route table size for easier troubleshooting and faster recovery from failures

Step 5: In **Configuration > Device Setup > Routing > EIGRP > Summary Address**, click **Add**.

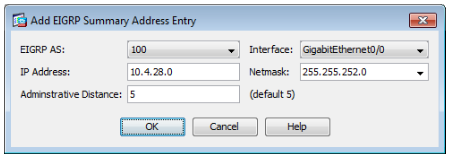
Step 6: In the **Add EIGRP Summary Address Entry** dialog box, in the **Interface** list, select **GigabitEthernet0/0**.

Step 7: In the **IP Address** box, enter the remote-access pool's summary network address. (Example: 10.4.28.0)

Step 8: Enter the summary **Netmask**. (Example 255.255.252.0)

Step 9: In the **Administrative Distance** box, enter **5**, and then click **OK**.

Step 10: On the Summary Address pane, click **Apply**.



Add EIGRP Summary Address Entry

EIGRP AS: 100 Interface: GigabitEthernet0/0

IP Address: 10.4.28.0 Netmask: 255.255.252.0

Adminstrative Distance: 5 (default 5)

Next, you will allow intra-interface traffic. This is critical to allow VPN users (specifically remote workers with unified communications software clients) to communicate with each other.

Step 11: Navigate to **Configuration > Device Setup > Interfaces**.

Step 12: Select **Enable traffic between two or more hosts connected to the same interface**, and then click **Apply**.

Procedure 3 Configure the group-URL

The Cisco 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 Cisco 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 to which they are assigned. Alternatively, the user can directly access the VPN group with the group-url, after which they will need to provide their username and password.

If using the Internet Edge 10K design with dual ISP connections, expect to offer VPN connectivity through both ISP connections, and be sure to provide group-urls for the IP address or host names for both ISPs.

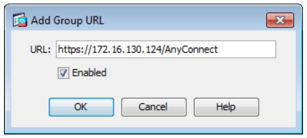
Step 1: Navigate to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**.

Step 2: In the **Connection Profiles** pane, select the profile created in the previous procedure (Example: AnyConnect), and then click **Edit**.

Step 3: On the **Edit AnyConnect Connect Profile** dialog box, navigate to **Advanced > Group Alias/Group URL**.

Step 4: On the **Group URLs** pane, click **Add**.

Step 5: In the **URL** box, enter the URL containing the firewall's primary Internet connection IP address and a user group string, and then click **OK**. (Example: https://172.16.130.134/AnyConnect)



URL: https://172.16.130.124/AnyConnect

☑ Enabled

Step 6: If you are using the Internet Edge 10k design, which has a resilient Internet connection, repeat Step 1- Step 5 using the firewall's resilient Internet connection IP address. (Example: https://172.17.130.124/AnyConnect)

If you are using the Internet Edge 5k design, advance to the next procedure.

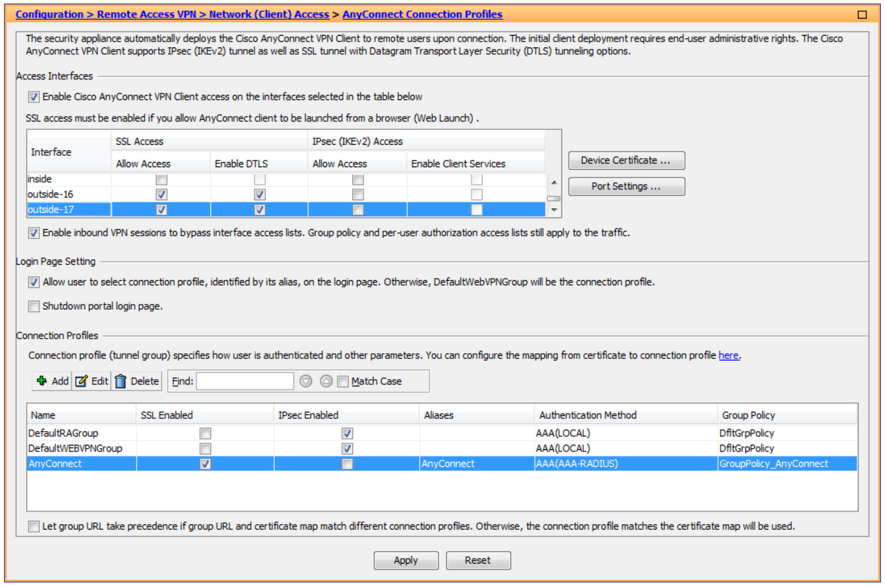
Procedure 4 Configure resilient Internet connection

(Optional)

Step 1: Navigate **to Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**.

Step 2: In the **Configuration** window, in the **Access Interfaces** pane, select the interface attached to the resilient Internet connection. (Example: outside-17)

Step 3: Under SSL Access, select **Allow Access**, and then click **Apply**.



The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.

Access Interfaces

☑ Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch) .

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
inside	☐	☐	☐	☐
outside-16	☑	☑	☐	☐
outside-17	☑	☑	☐	☐

☑ Enable inbound VPN sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.

Login Page Setting

☑ Allow user to select connection profile, identified by its alias, on the login page. Otherwise, DefaultWebVPNGroup will be the connection profile.

☐ Shutdown portal login page.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile here.

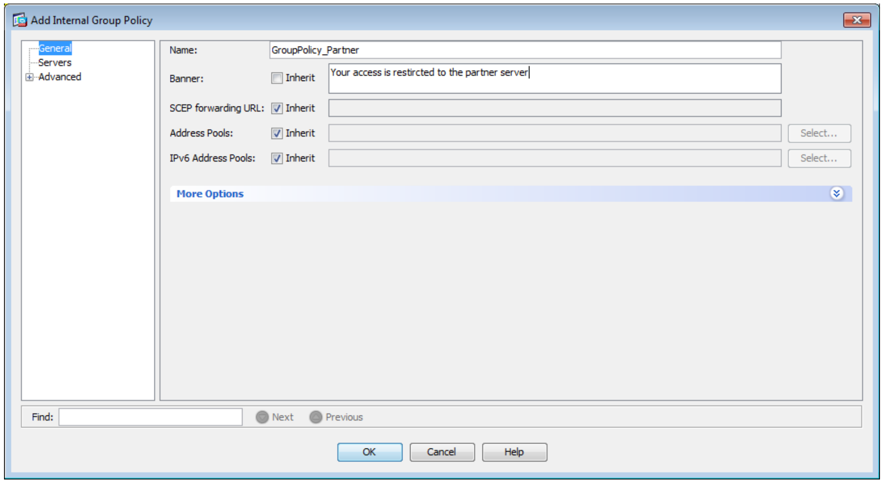
Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	☐	☑		AAA(LOCAL)	DfltGrpPolicy
DefaultWEBVPNGroup	☐	☑		AAA(LOCAL)	DfltGrpPolicy
AnyConnect	☑	☐	AnyConnect	AAA(AAA-RADIUS)	GroupPolicy_AnyConnect

☐ Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile matches the certificate map will be used.

Procedure 5 Configure the partner policy

Step 1: In **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**, click **Add**.

Step 2: On the **Add Internal Group Policy** dialog box, enter a **Name**. (Example: GroupPolicy_Partner)



Add Internal Group Policy

Name: GroupPolicy_Partner

Banner: □ Inherit Your access is restircted to the partner server

SCEP forwarding URL: ☑ Inherit

Address Pools: ☑ Inherit

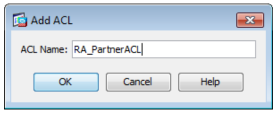
IPv6 Address Pools: ☑ Inherit

Step 3: Click the two down arrows. The **More Options** pane expands.

Step 4: For **IPv4 Filter**, clear **Inherit**, and then click **Manage**.

Step 5: On the **ACL Manager** dialog box, click **Add > Add ACL**.

Step 6: In the **Add ACL** dialog box, enter an **ACL Name**, and then click **OK**. (Example RA_PartnerACL)



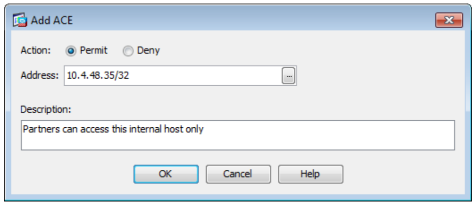
Add ACL

ACL Name: RA_PartnerACL

Step 7: Click **Add > Add ACE**.

Step 8: In the **Add ACE** dialog box, for **Action**, select **Permit**.

Step 9: In the **Address** box, enter the IP address and netmask which the partner will be allowed to access, and then click **OK**. (Example: 10.4.48.35/32)



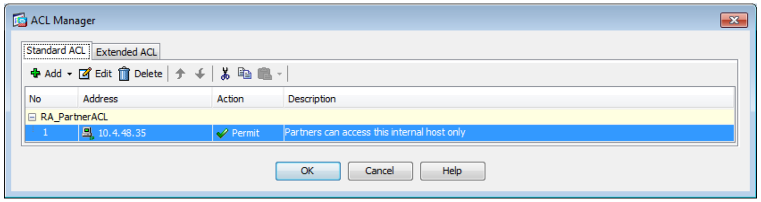
Add ACE

Action: ● Permit ○ Deny

Address: 10.4.48.35/32

Description:
Partners can access this internal host only

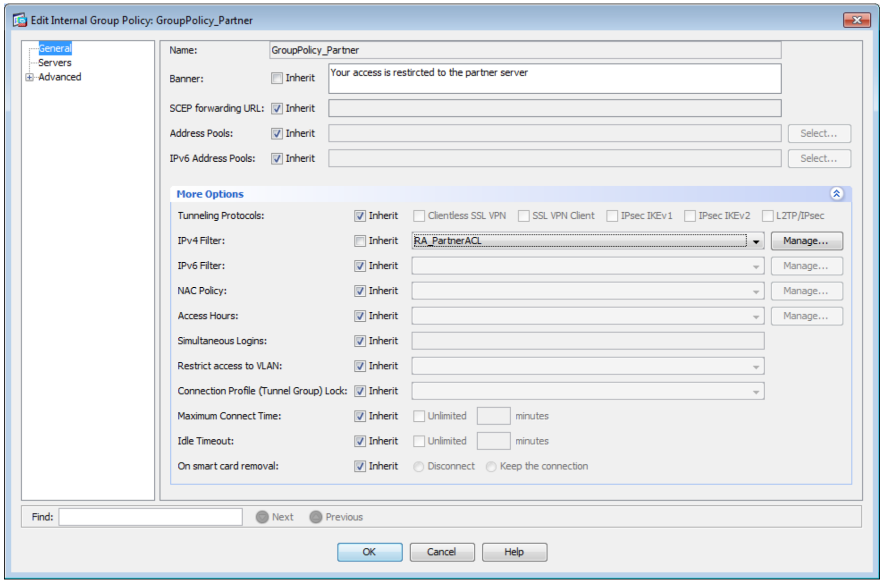
Step 10: In the **ACL Manager** dialog box, click **OK**.



ACL Manager

No	Address	Action	Description
RA_PartnerACL			
1	10.4.48.35	✓ Permit	Partners can access this internal host only

Step 11: In the **Add Internal Group Policy** dialog box, click **OK**.



Edit Internal Group Policy: GroupPolicy_Partner

Name: GroupPolicy_Partner

Banner: □ Inherit Your access is restircted to the partner server

SCEP forwarding URL: ☑ Inherit

Address Pools: ☑ Inherit

IPv6 Address Pools: ☑ Inherit

More Options

Tunneling Protocols: ☑ Inherit □ Clientless SSL VPN □ SSL VPN Client □ IPsec IKEv1 □ IPsec IKEv2 □ L2TP/IPsec

IPv4 Filter: □ Inherit RA_PartnerACL

IPv6 Filter: ☑ Inherit

NAC Policy: ☑ Inherit

Access Hours: ☑ Inherit

Simultaneous Logins: ☑ Inherit

Restrict access to VLAN: ☑ Inherit

Connection Profile (Tunnel Group) Lock: ☑ Inherit

Maximum Connect Time: ☑ Inherit □ Unlimited minutes

Idle Timeout: ☑ Inherit □ Unlimited minutes

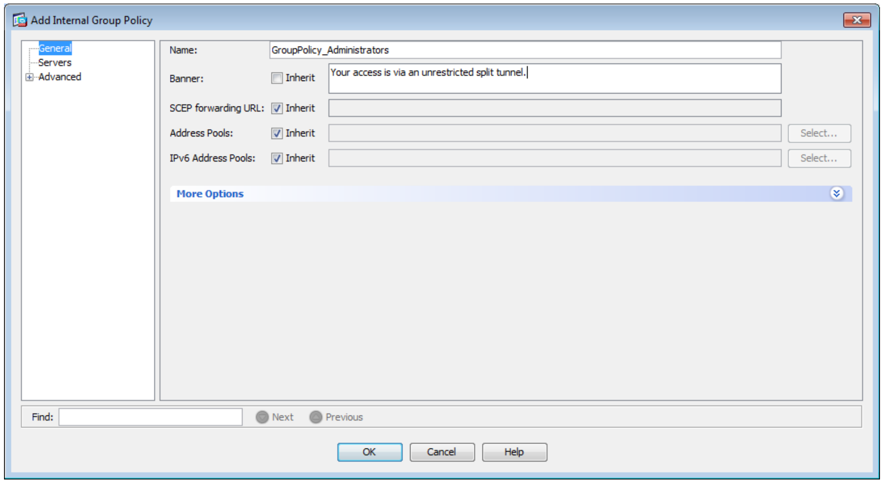
On smart card removal: ☑ Inherit ○ Disconnect ○ Keep the connection

Step 12: On the Group Policies pane, click **Apply**.

Procedure 6 Configure the admin policy

Step 1: In **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**, click **Add**.

Step 2: On the **Add Internal Group Policy** dialog box, enter a **Name**. (Example: GroupPolicy_Administrators)



Add Internal Group Policy

Name: GroupPolicy_Administrators

Banner: □ Inherit Your access is via an unrestricted split tunnel.

SCEP forwarding URL: ☑ Inherit

Address Pools: ☑ Inherit

IPv6 Address Pools: ☑ Inherit

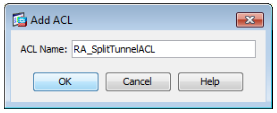
Step 3: In the navigation tree, click **Advanced > Split Tunneling**.

Step 4: For **Policy**, clear **Inherit**, and then select **Tunnel Network List Below**.

Step 5: For **Network List**, clear **Inherit**, and then click **Manage**.

Step 6: On the **ACL Manager** dialog box, click **Add > Add ACL**.

Step 7: In the **Add ACL** dialog box, enter an **ACL Name**, and then click **OK**. (Example RA_SplitTunnelACL)



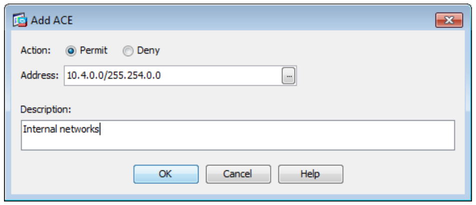
Add ACL

ACL Name: RA_SplitTunnelACL

Step 8: Click **Add > Add ACE**.

Step 9: In the **Add ACE** dialog box, for **Action**, select **Permit**.

Step 10: In the **Address** box, enter the internal summary IP address and netmask, and then click **OK**. (Example: 10.4.0.0/255.254.0.0)



Add ACE

Action: ● Permit ○ Deny

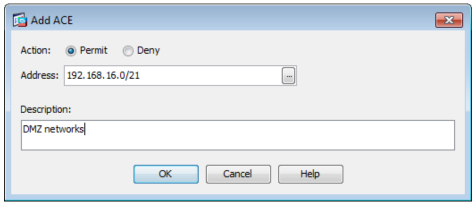
Address: 10.4.0.0/255.254.0.0

Description: Internal networks

Step 11: Click **Add > Add ACE**.

Step 12: In the **Add ACE** dialog box, for **Action**, select **Permit**.

Step 13: In the **Address** box, enter the DMZ summary IP address and netmask, and then click **OK**. (Example: 192.168.16.0/21)



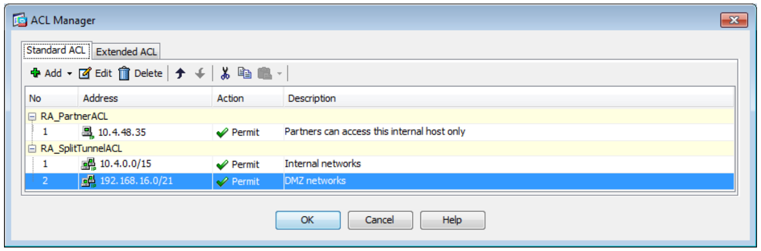
Add ACE

Action: ● Permit ○ Deny

Address: 192.168.16.0/21

Description: DMZ networks

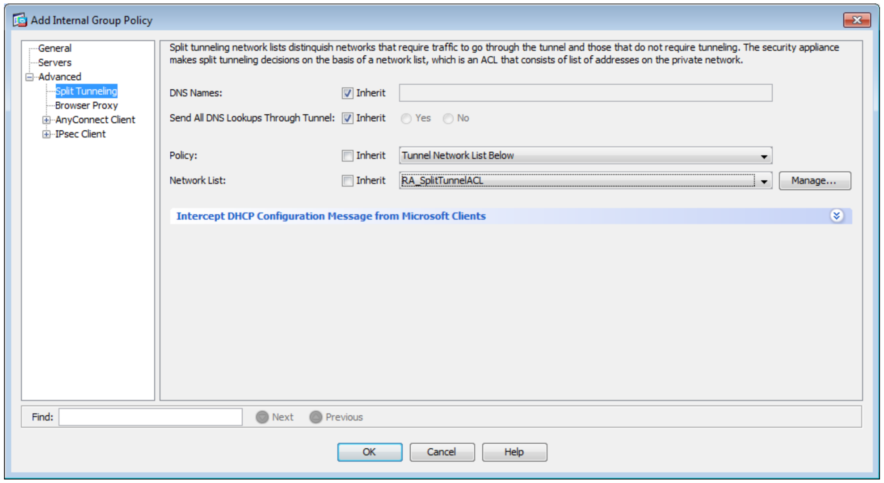
Step 14: In the **ACL Manager** dialog box, click **OK**.



ACL Manager

No	Address	Action	Description
RA_PartnerACL			
1	10.4.48.35	✓ Permit	Partners can access this internal host only
RA_SplitTunnelACL			
1	10.4.0.0/15	✓ Permit	Internal networks
2	192.168.16.0/21	✓ Permit	DMZ networks

Step 15: In the **Add Internal Group Policy** dialog box, click **OK**.



Add Internal Group Policy

Split tunneling network lists distinquish networks that require traffic to go through the tunnel and those that do not require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, which is an ACL that consists of list of addresses on the private network.

DNS Names: ☑ Inherit

Send All DNS Lookups Through Tunnel: ☑ Inherit ○ Yes ○ No

Policy: □ Inherit Tunnel Network List Below

Network List: □ Inherit RA_SplitTunnelACL

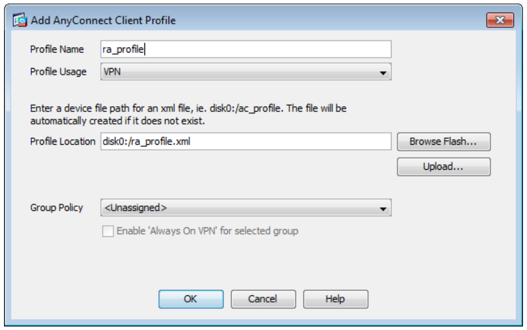
Step 16: On the Group Policies pane, click **Apply**.

Procedure 7 Cisco AnyConnect Client Profile

Cisco AnyConnect Client Profile is the location where some of the newer configuration of the Cisco AnyConnect client is defined. Cisco AnyConnect 2.5 and later use the configuration in this section, including many of the newest features added to the Cisco AnyConnect client.

Step 1: In **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**, click **Add**.

Step 2: In the **Add AnyConnect Client Profile** dialog box, in the **Profile Name** box, enter **ra_profile**, and then click **OK** and **Apply**.



Add AnyConnect Client Profile

Profile Name: ra_profile

Profile Usage: VPN

Enter a device file path for an xml file, ie. disk0:/ac_profile. The file will be automatically created if it does not exist.

Profile Location: disk0:/ra_profile.xml

Group Policy: <Unassigned>

□ Enable 'Always On VPN' for selected group

Step 3: On the AnyConnect Client Profile pane, select the ra_profile you just built, and then click **Edit**.

The **Server List Panel** allows you to enter names and addresses for the appliances to which the Cisco AnyConnect Client is allowed to connect.

Step 4: Click **Server List > Add**.

Step 5: In the **Server List Entry** dialog box, in the **Hostname** box, enter the name of the remote-access firewall. (Example: IE-ASA5540)

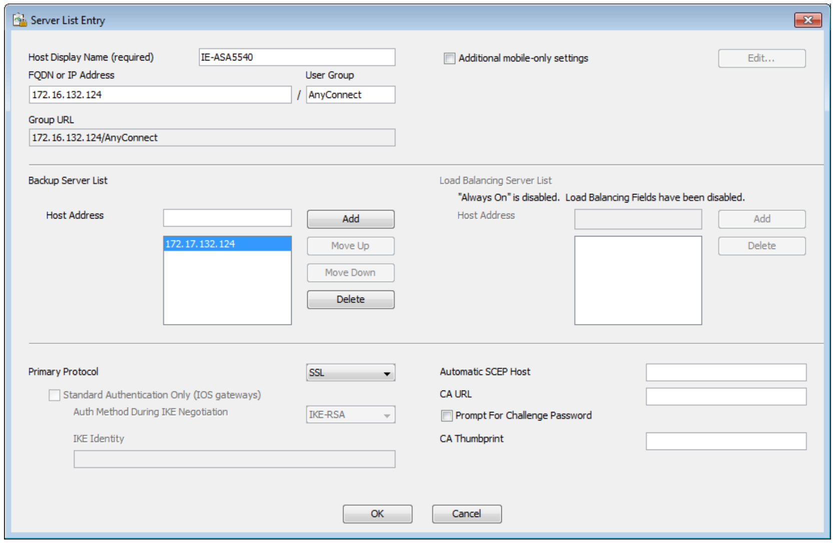
Step 6: In the **FQDN or IP Address** box, enter the firewall's primary Internet connection IP address. (Example: 172.16.132.124)

Step 7: In the **User Group** box, enter the name defined in Procedure 3. (Example: AnyConnect)

Step 8: If you are using the Internet Edge 10k design, in the **Host Address** box, enter the firewall's resilient Internet connection IP address, and then click **Add**. (Example: 172.17.132.124)

If you are using the Internet Edge 5k design, proceed to the next step.

Step 9: Click **OK**.



Server List Entry

Host Display Name (required): IE-ASA5540

□ Additional mobile-only settings

FQDN or IP Address: 172.16.132.124 / User Group: AnyConnect

Group URL: 172.16.132.124/AnyConnect

Backup Server List

Host Address: 172.17.132.124

Load Balancing Server List

"Always On" is disabled. Load Balancing Fields have been disabled.

Primary Protocol: SSL

□ Standard Authentication Only (IOS gateways)

Auth Method During IKE Negotiation: IKE-RSA

IKE Identity

Automatic SCEP Host

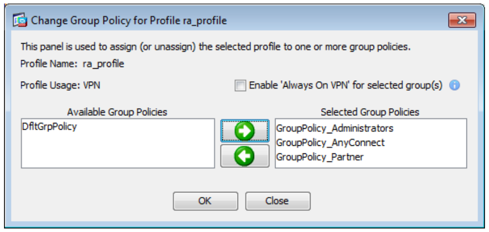
CA URL

□ Prompt For Challenge Password

CA Thumbprint

Step 10: On the AnyConnect Client Profile pane, click **Change Group Policy**.

Step 11: In the **Change Group Policy for Profile** dialog box, select the three group policies you just created in the available group policies list, click the right arrow, and then click **OK**.



Change Group Policy for Profile ra_profile

This panel is used to assign (or unassign) the selected profile to one or more group policies.

Profile Name: ra_profile

Profile Usage: VPN

□ Enable 'Always On VPN' for selected group(s)

Available Group Policies: DfltGrpPolicy

Selected Group Policies: GroupPolicy_Administrators, GroupPolicy_AnyConnect, GroupPolicy_Partner

Step 12: On the AnyConnect Client Profile pane, click **Apply**.

Notes

Email Security

Business Overview

Email is a critical business service in most organizations. 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, waste employee time (because of the sheer volume of messages) and waste network bandwidth and storage.

Another problem is that large numbers of email 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

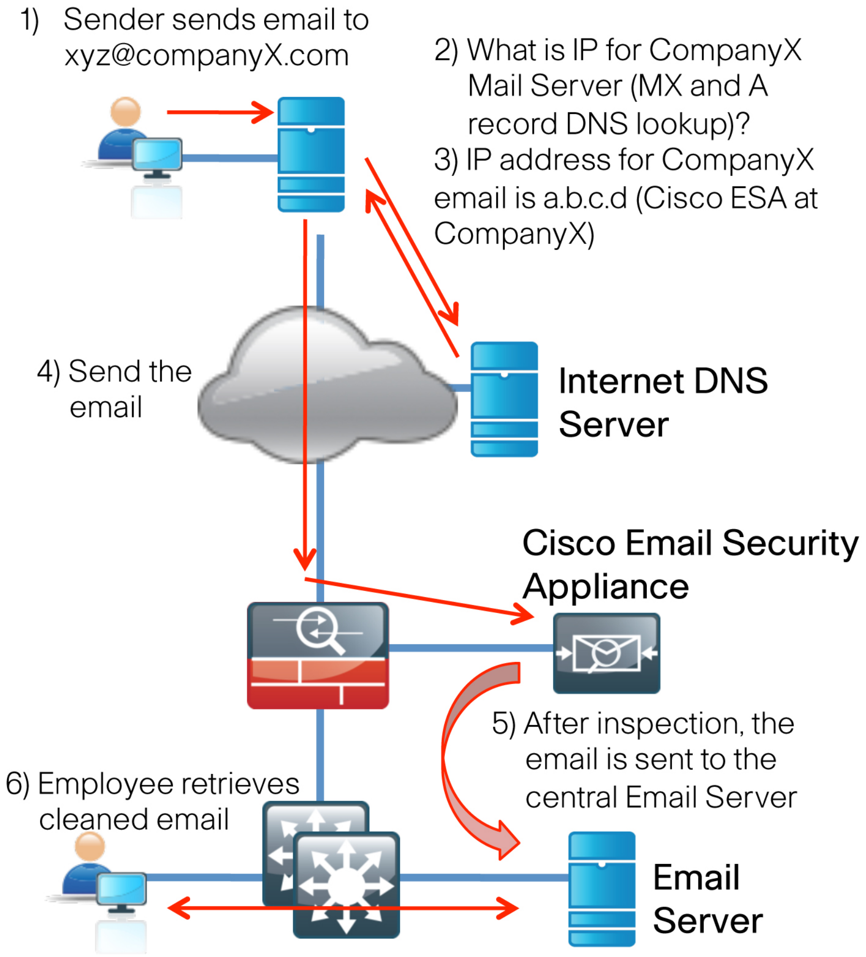
An email solution will become unusable if junk email is not filtered properly. The sheer volume of junk messages crowd out legitimate mail and cause employees to waste time manually filtering through messages. A side effect of some junk email-filtering solutions are false positives, or email that is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

When this occurs, the organization 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 and making the user responsible for determining whether email is spam. Unsolicited email is also more likely to be malicious and include embedded attacks. Criminal organizations 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 attempts to infect the host machine or that offers 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 is to gather social security numbers and credit card numbers or to compromise the host in order to use it as a launch point to send spam and other attacks.

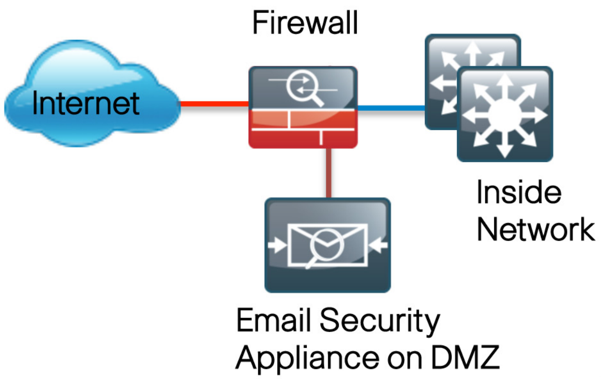
The Cisco IronPort Email Security Appliance (ESA) protects the email infrastructure and employees who use email at work by filtering unsolicited and malicious email before it reaches the user. IronPort ESA easily integrates into existing email infrastructures with a high degree of flexibility. It does 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 in which an organization is using an MTA might look like the message flow shown below.

Figure 15 - Email message flow


1) Sender sends email to xyz@companyX.com
2) What is IP for CompanyX Mail Server (MX and A record DNS lookup)?
3) IP address for CompanyX email is a.b.c.d (Cisco ESA at CompanyX)
4) Send the email
Internet DNS Server
Cisco Email Security Appliance
5) After inspection, the email is sent to the central Email Server
6) Employee retrieves cleaned email
Email Server

IronPort ESA can be deployed with a single physical interface in order to filter email to and from an organization'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 16 - Cisco IronPort Email Security Appliance deployment overview



IronPort 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 that use reputation, such as IronPort ESA, get updates several times a day from SenderBase. When IronPort ESA receives an email, it compares the source IP to the database provided by SenderBase. If the reputation of the sender is positive, IronPort ESA forwards the email on to the next layer of defense. If the reputation is negative, IronPort ESA discards the email. If the reputation falls in between, the email is considered suspicious, IronPort ESA quarantines the email, and waits for inspection before delivering or discarding the email.

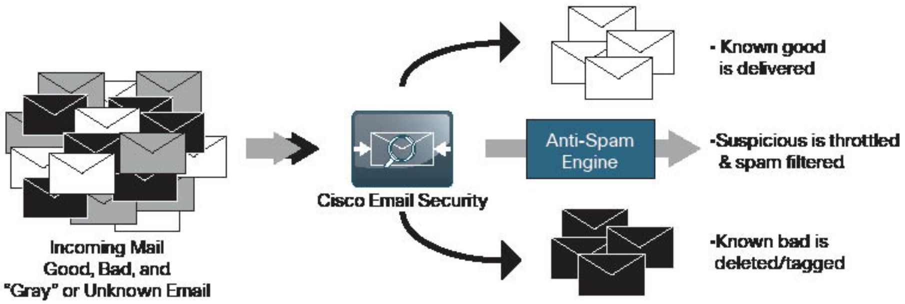
Context-based antispam inspection in IronPort ESA inspects the entire mail message, including attachments, looking for details like sender identity, message content, embedded URLs, and email formatting. Using these algorithms, IronPort ESA can identify spam messages without blocking legitimate email.

Cisco IronPort Email Security Appliance uses a multilayer approach to fight viruses. The first layer is the Virus Outbreak Filters. The appliance downloads Virus Outbreak Filters from SenderBase. They contain a list of known-bad mail servers. These filters are generated by watching for anomalies associated with an outbreak in global email traffic patterns.

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.

IronPort ESA is antivirus (AV) signatures to scan quarantined email to ensure that they do not carry viruses into the network.

Figure 17 - Email Filtering Overview


Incoming Mail
Good, Bad, and
"Gray" or Unknown Email
Cisco Email Security
Anti-Spam Engine
- Known good is delivered
-Suspicious is throttled & spam filtered
-Known bad is deleted/tagged

Deployment 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 organization; as such, the public MX records (the DNS record that defines where to send mail) must eventually point to the public IP address of 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.

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.

Process

Email DMZ Configuration

1. Configure the DMZ switch
2. Configure Demilitarized Zone interface
3. Configure Network Address Translation
4. Configure security policy

The firewall's demilitarized zone (DMZ) is a portion of the network where, typically, traffic to and from other parts of the network is tightly restricted. Organizations 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.

In this process, a DMZ for the ESA is configured so it can serve as the organization's MTA for email sent via the Internet.

Procedure 1 Configure the DMZ switch

Step 1: Set the DMZ switch to be the spanning tree root for the VLAN that contains the email security appliance.

```
vlan 1117
spanning-tree vlan 1117 root primary
```

Step 2: Configure the interfaces that connect to the appliances..

```
interface GigabitEthernet1/0/24
 description IE-ASA5540a Gig0/1
!
interface GigabitEthernet1/0/24
 description IE-ASA5540b Gig0/1
!
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan add 1117
 switchport mode trunk
 macro apply EgressQoS
 logging event link-status
 logging event trunk-status
 no shutdown
```

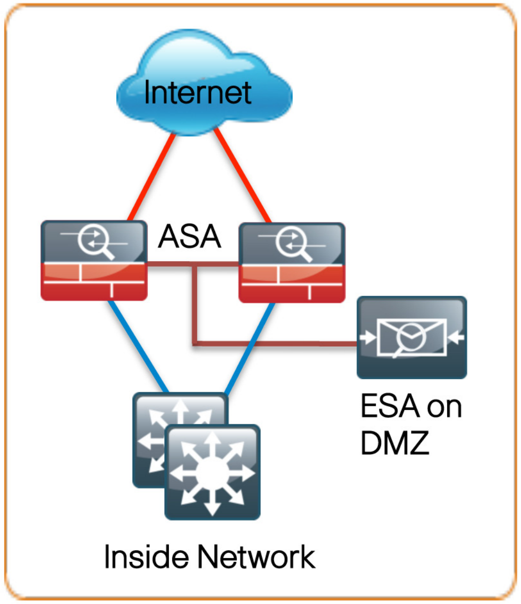
Step 3: Configure the interfaces that are connected to the email security appliance.

```
interface GigabitEthernet1/0/22
 description DMZ-ESAc370
 switchport access vlan 1117
 switchport host
 macro apply EgressQoS
 logging event link-status
 no shutdown
```

Procedure 2 Configure Demilitarized Zone interface

The DMZ network is connected to the appliances on the appliances' GigabitEthernet interface via a VLAN trunk in order to allow the greatest flexibility if new VLANs must be added to connect additional DMZs. The trunk connects the appliances to a 3750x access-switch stack in order to provide resiliency. The DMZ VLAN interfaces on the Cisco ASA are each assigned an IP address that isthe 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, except for one VLAN interface with an IP address for management of the switch.

Figure 18 - DMZ VLAN topology and services



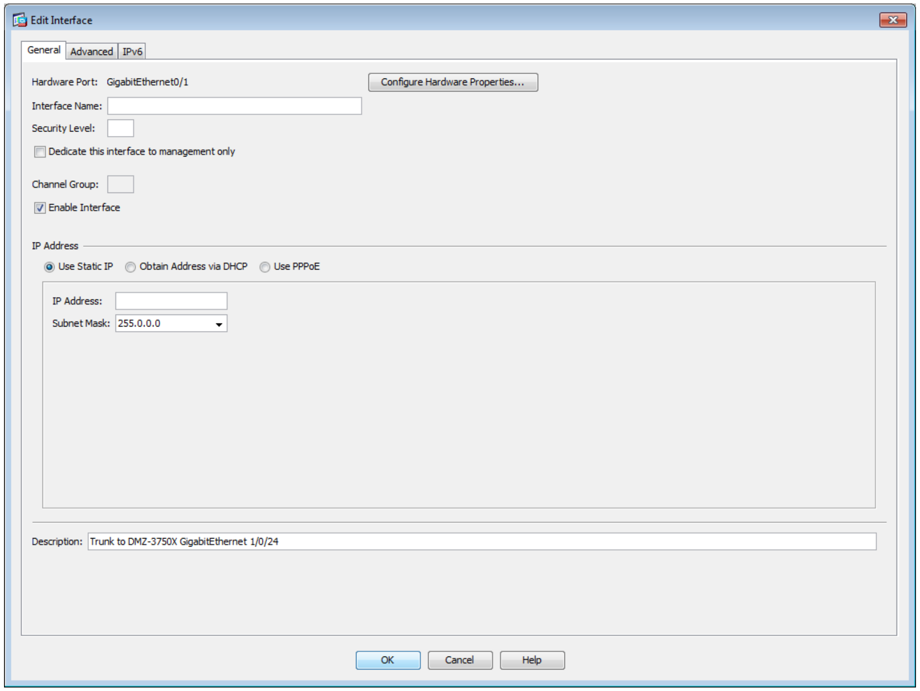
Tech Tip

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

Step 1: In **Configuration > Device Setup > Interfaces**, click the interface that is connected to the DMZ switch. (Example: GigabitEthernet0/1)

Step 2: Click **Edit**.

Step 3: In the **Edit Interface** dialog box, select **Enable Interface**, and then click **OK**.



Hardware Port: GigabitEthernet0/1

Interface Name:

Security Level:

☐ Dedicate this interface to management only

Channel Group:

☑ Enable Interface

IP Address

● Use Static IP ○ Obtain Address via DHCP ○ Use PPPoE

IP Address:

Subnet Mask: 255.0.0.0

Description: Trunk to DMZ-3750X GigabitEthernet 1/0/24

Step 4: On the **Interface** pane, click **Add > Interface**.

Step 5: In the **Add Interface** dialog box, in the **Hardware Port** list, select the interface configured in Step 1.(Example: GigabitEthernet0/1)

Step 6: In the **VLAN ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1117)

Step 7: In the **Subinterface ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1117)

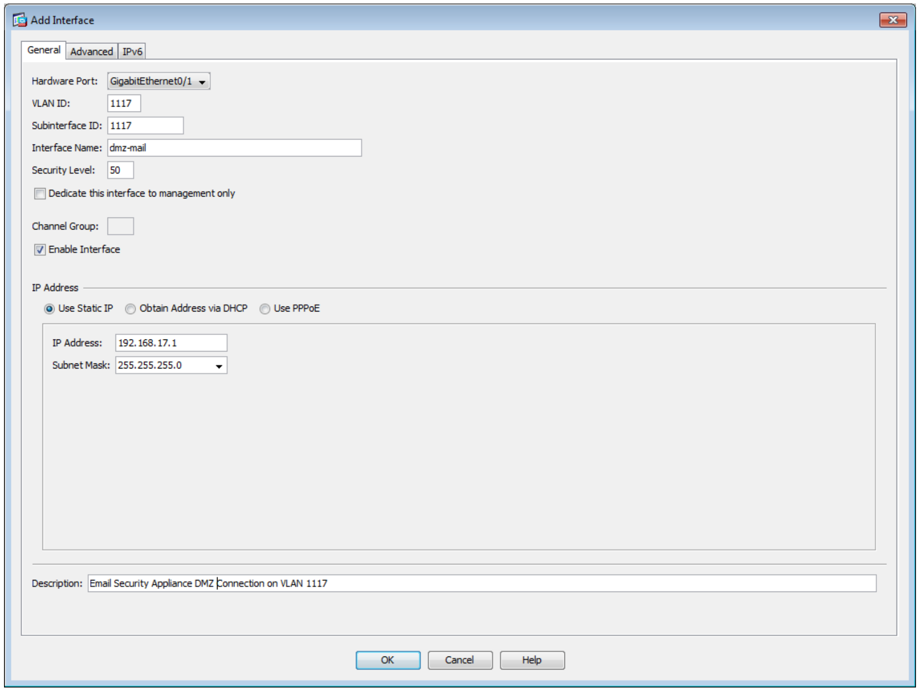
Step 8: Enter an **Interface Name**. (Example: dmz-email)

Step 9: In the **Security Level** box, enter a value of **50**.

Step 10: Enter the interface **IP Address**. (Example: 192.168.17.1)

Step 11: Enter the interface **Subnet Mask**, and then click **OK**. (Example: 255.255.255.0)

Step 12: On the **Interface** pane, click **Apply**.



Hardware Port:	GigabitEthernet0/1
VLAN ID:	1117
Subinterface ID:	1117
Interface Name:	dmz-mail
Security Level:	50

☐ Dedicate this interface to management only

Channel Group:

☑ Enable Interface

IP Address

● Use Static IP ○ Obtain Address via DHCP ○ Use PPPoE

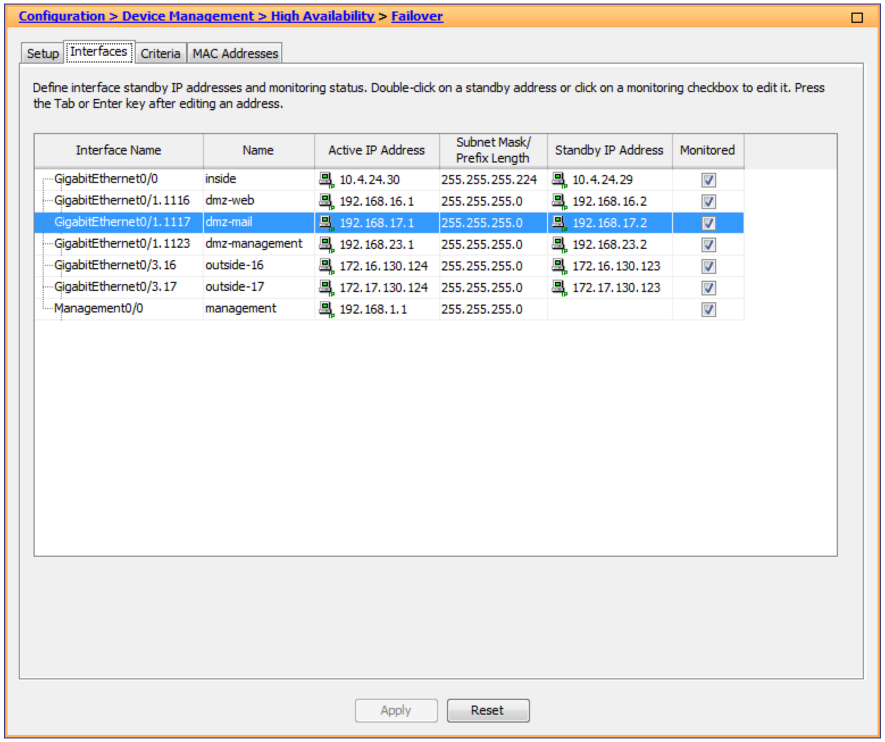
IP Address:	192.168.17.1
Subnet Mask:	255.255.255.0

Description: Email Security Appliance DMZ Connection on VLAN 1117

Step 13: Navigate to **Configuration > Device Management > High Availability > Failover.**

Step 14: On the **Interfaces** tab, in the **Standby IP address** column, enter the IP address of the standby unit for the interface you just created. (Example: 192.168.17.2)

Step 15: Select **Monitored**, and then click **Apply**.



Configuration > Device Management > High Availability > Failover
Setup | Interfaces | Criteria | MAC Addresses

Define interface standby IP addresses and monitoring status. Double-click on a standby address or click on a monitoring checkbox to edit it. Press the Tab or Enter key after editing an address.

Interface Name	Name	Active IP Address	Subnet Mask/ Prefix Length	Standby IP Address	Monitored
GigabitEthernet0/0	inside	10.4.24.30	255.255.255.224	10.4.24.29	☑
GigabitEthernet0/1.1116	dmz-web	192.168.16.1	255.255.255.0	192.168.16.2	☑
GigabitEthernet0/1.1117	dmz-mail	192.168.17.1	255.255.255.0	192.168.17.2	☑
GigabitEthernet0/1.1123	dmz-management	192.168.23.1	255.255.255.0	192.168.23.2	☑
GigabitEthernet0/3.16	outside-16	172.16.130.124	255.255.255.0	172.16.130.123	☑
GigabitEthernet0/3.17	outside-17	172.17.130.124	255.255.255.0	172.17.130.123	☑
Management0/0	management	192.168.1.1	255.255.255.0		☑

Procedure 3 Configure Network Address Translation

The DMZ network uses private network (RFC 1918) addressing that is not Internet routable, so the firewall must translate the DMZ address of the IronPort ESA to an outside public address. If there is a resilient Internet connection, the IronPort ESA can have an address translation for each ISP. This resilient configuration, shown here for completeness, relies on the modification of DNS records to point incoming requests to the resilient IronPort ESA when the primary Internet connection is unavailable.

The example DMZ address to public IP address mapping is shown in the following table.

Table 6 - IronPort ESA address mapping

IronPort ESA DMZ Address	IronPort ESA Public Address (externally routable after NAT)
192.168.17.25	172.16.130.25 (ISP-A)
	172.17.130.25 (ISP-B)

Step 1: Navigate to **Configuration > Firewall > Objects > Network Objects/Groups**.

First, you will add a network object for the public address of the IronPort ESA server on the primary Internet connection.

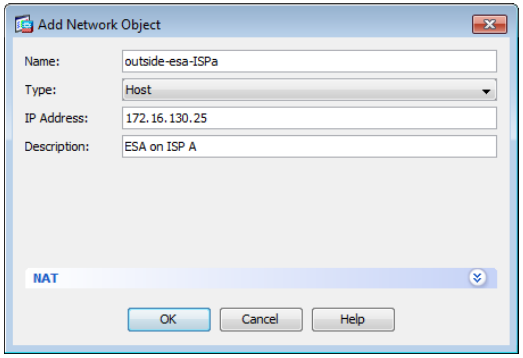
Step 2: Click **Add > Network Object**.

Step 3: On **the Add Network Object** dialog box, in the **Name box**, enter a description for the IronPort ESA's public IP address. (Example: outside-esa-ISPa)

Step 4: In the **Type** list, select **Host**.

Step 5: In the **IP Address** box, enter the IronPort ESA's public IP address, and then click **OK**. (Example: 172.16.130.25)

Step 6: On the **Network Objects/Groups** pane, click **Apply**.


Add Network Object

Name: outside-esa-ISPa

Type: Host

IP Address: 172.16.130.25

Description: ESA on ISP A

Next, you will add a network object for the private DMZ address of the IronPort ESA.

Step 7: Click **Add > Network Object**.

Step 8: On the **Add Network Object** dialog box, in the **Name box**, enter a description for the IronPort ESA's private DMZ IP address. (Example: dmz-esa-ISPa)

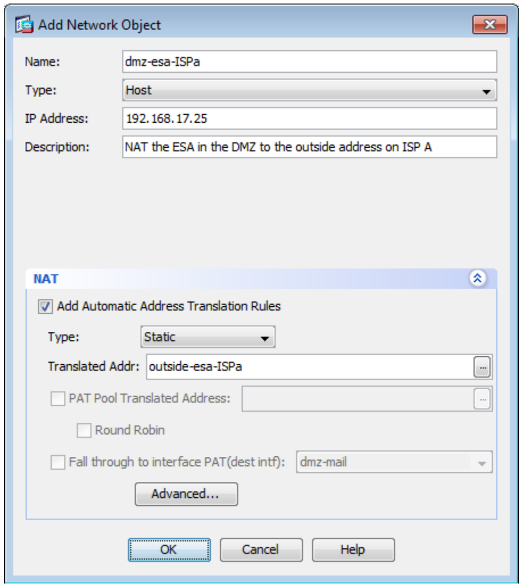
Step 9: In the **Type** list, select **Host**.

Step 10: In the **IP Address** box, enter the primary wireless LAN controller's private DMZ IP address. (Example: 192.168.17.25)

Step 11: Click the two down arrows. The NAT pane expands.

Step 12: Select **Add Automatic Address Translation Rules**.

Step 13: In the **Translated Addr** list, select the network object created in Step 2.


Add Network Object

Name: dmz-esa-ISPa

Type: Host

IP Address: 192.168.17.25

Description: NAT the ESA in the DMZ to the outside address on ISP A

NAT

☑ Add Automatic Address Translation Rules

Type: Static

Translated Addr: outside-esa-ISPa

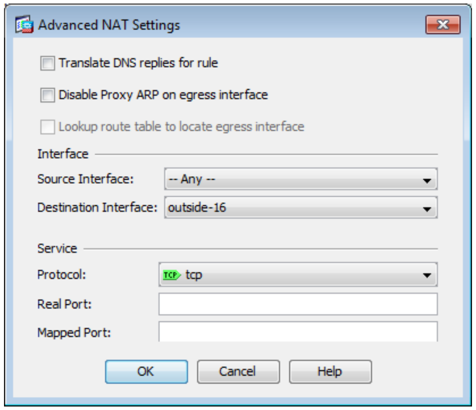
□ PAT Pool Translated Address:

□ Round Robin

□ Fall through to interface PAT(dest intf): dmz-mail

Step 14: Click **Advanced**.

Step 15: In the **Advanced NAT Settings** dialog box, in the **Destination Interface** list, select the interface name for the primary Internet connection, and then click **OK**. (Example: outside-16)


Advanced NAT Settings

□ Translate DNS replies for rule

□ Disable Proxy ARP on egress interface

□ Lookup route table to locate egress interface

Interface

Source Interface: -- Any --

Destination Interface: outside-16

Service

Protocol: tcp

Real Port:

Mapped Port:

Step 16: In the **Add Network Object** dialog box, click **OK**.

Step 17: On the **Network Objects/Groups** pane, click **Apply**.

Step 18: If you are using the Internet Edge 10k design, which has a resilient Internet connection, repeat this procedure for the resilient Internet connection.

If you are using the Internet Edge 5k design, advance to the next procedure.

Procedure 4 Configure security policy

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. The security policy allows only mail traffic to the IronPort ESA. The IronPort 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 IronPort ESA is allowed to make inbound SMTP connections to the corporate exchange server as well as DNS requests to the organization's DNS server.

First, you ease the configuration of the security policy by creating two network objects that summarize all the DMZ networks. All the DMZ networks deployed in SBA for Enterprise can be summarized as 192.168.16.0/21.

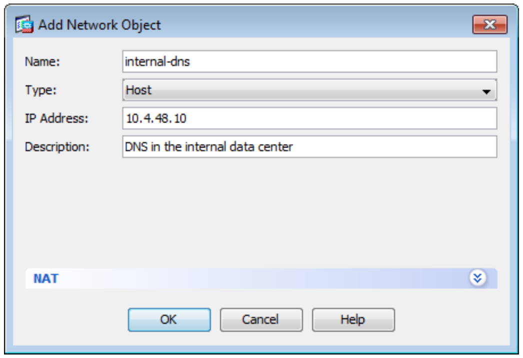
Step 1: Navigate to **Configuration > Firewall > Objects > Network Objects/Groups**.

Step 2: Click **Add > Network Object**.

Step 3: On the **Add Network Object** dialog box, in the **Name box**, enter a description. (Example: internal-dns)

Step 4: In the **Type** list, select **Host**.

Step 5: In the **IP Address** box, enter the address of the internal DNS, and then click **OK**. (Example: 10.4.48.10)



Add Network Object

Name: internal-dns

Type: Host

IP Address: 10.4.48.10

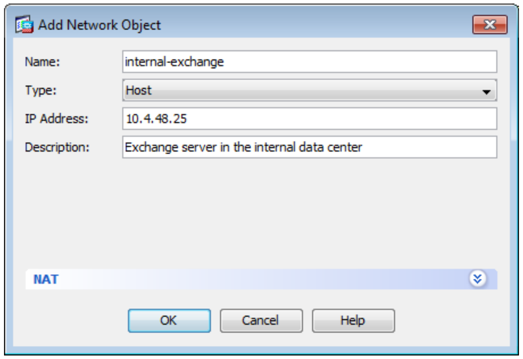
Description: DNS in the internal data center

Step 6: Click **Add > Network Object**.

Step 7: On the **Add Network Object** dialog box, in the **Name box**, enter a description. (Example: internal-exchange)

Step 8: In the **Type** list, select **Host**.

Step 9: In the **IP Address** box, enter the address of the internal Microsoft Exchange server, and then click **OK**. (Example: 10.4.48.25)



Add Network Object

Name: internal-exchange

Type: Host

IP Address: 10.4.48.25

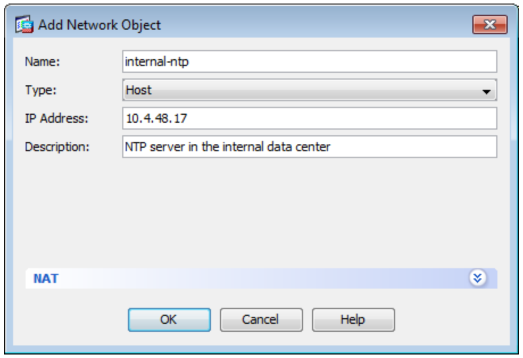
Description: Exchange server in the internal data center

Step 10: Click **Add > Network Object**.

Step 11: On the **Add Network Object** dialog box, in the **Name box**, enter a description. (Example: internal-ntp)

Step 12: In the **Type** list, select **Host**.

Step 13: In the **IP Address** box, enter the address of the internal NTP server, and then click **OK**. (Example: 10.4.48.17)



Add Network Object

Name: internal-ntp

Type: Host

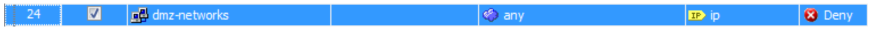
IP Address: 10.4.48.17

Description: NTP server in the internal data center

Step 14: On the **Network Objects/Groups** pane, click **Apply**.

Step 15: Navigate to **Configuration > Firewall > Access Rules**.

Step 16: Click the rule that denies traffic from the DMZ toward the internal network.



24 ☑ dmz-networks | | any | ip | Deny

Next, you will insert a new rule above the rule you selected that permits the ESA to receive email.

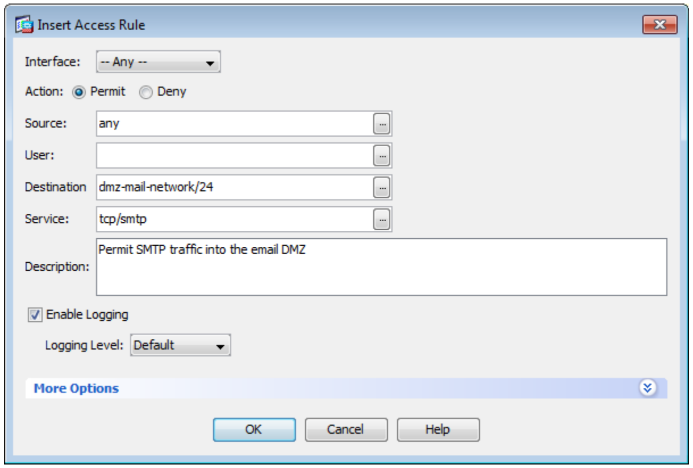
Step 17: Click **Add > Insert**.

Step 18: In the **Add Access Rule** dialog box, in the **Interface** list, select **—Any—**.

Step 19: For **Action**, select **Permit**.

Step 20: In the **Destination** list, select the network object automatically created for the email DMZ. (Example: dmz-mail-network/24)

Step 21: In the **Service** list, enter **tcp/smtp**, and then click **OK**.



Insert Access Rule

Interface: -- Any --

Action: ● Permit ○ Deny

Source: any

User:

Destination dmz-mail-network/24

Service: tcp/smtp

Description: Permit SMTP traffic into the email DMZ

☑ Enable Logging

Logging Level: Default

Next, you will insert a new rule above the rule you selected that permits the ESA to transfer email to the internal email server.

Step 22: Click **Add > Insert**.

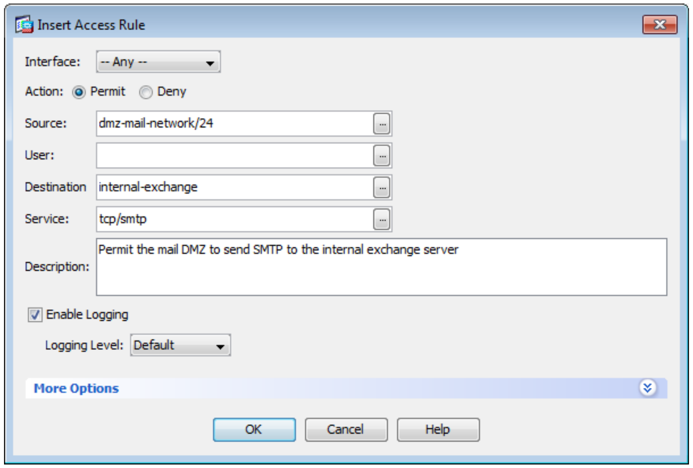
Step 23: In the **Insert Access Rule** dialog box, in the **Interface** list, select **—Any—**.

Step 24: For **Action**, select **Permit**.

Step 25: In the **Source** list, select the network object automatically created for the email DMZ. (Example: dmz-email-network/24)

Step 26: In the **Destination** list, select the internal Microsoft Exchange server network object. (Example: internal-exchange)

Step 27: In the **Service** list, enter **tcp/smtp**, and then click **OK**.



Insert Access Rule

Interface: -- Any --

Action: ● Permit ○ Deny

Source: dmz-mail-network/24

User:

Destination internal-exchange

Service: tcp/smtp

Description: Permit the mail DMZ to send SMTP to the internal exchange server

☑ Enable Logging

Logging Level: Default

Next, you will insert a new rule above the rule you selected the permits the ESA to perform domain lookups on the internal DNS.

Step 28: Click **Add > Insert**.

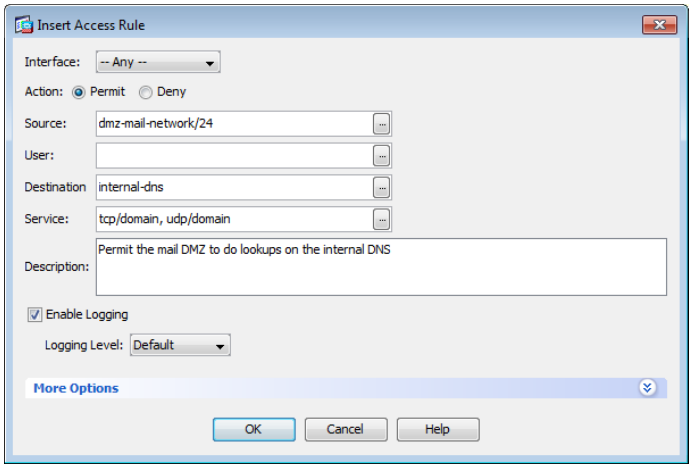
Step 29: In the **Insert Access Rule** dialog box, in the **Interface** list, select **—Any—**.

Step 30: For **Action**, select **Permit**.

Step 31: In the **Source** list, select the network object automatically created for the email DMZ. (Example: dmz-email-network/24)

Step 32: In the **Destination** list, select the internal DNS server network object. (Example: internal-dns)

Step 33: In the **Service** list, enter **tcp/domin, udp/domain**, and then click **OK**.



Interface: -- Any --

Action: ● Permit ○ Deny

Source: dmz-mail-network/24

User:

Destination: internal-dns

Service: tcp/domain, udp/domain

Description: Permit the mail DMZ to do lookups on the internal DNS

☑ Enable Logging

Logging Level: Default

Next, you will insert a new rule above the rule you selected that permits the ESA to update its clock using the internal NTP server.

Step 34: Click **Add > Insert**.

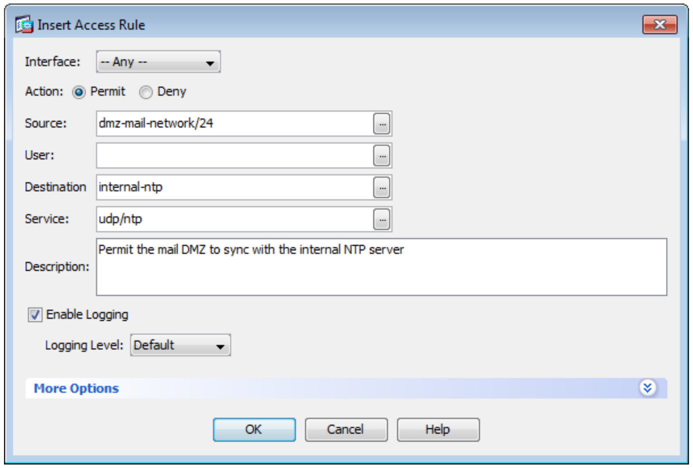
Step 35: In the **Insert Access Rule** dialog box, in the **Interface** list, select **—Any—**.

Step 36: For **Action**, select **Permit**.

Step 37: In the **Source** list, select the network object automatically created for the email DMZ. (Example: dmz-email-network/24)

Step 38: In the **Destination** list, select the internal NTP server network object. (Example: internal-ntp)

Step 39: In the **Service** list, enter **udp/ntp**, and then click **OK**.



Interface: -- Any --

Action: ● Permit ○ Deny

Source: dmz-mail-network/24

User:

Destination: internal-ntp

Service: udp/ntp

Description: Permit the mail DMZ to sync with the internal NTP server

☑ Enable Logging

Logging Level: Default

Next, you will insert a new rule above the rule you selected that permits the ESA to update its software and feature keys.

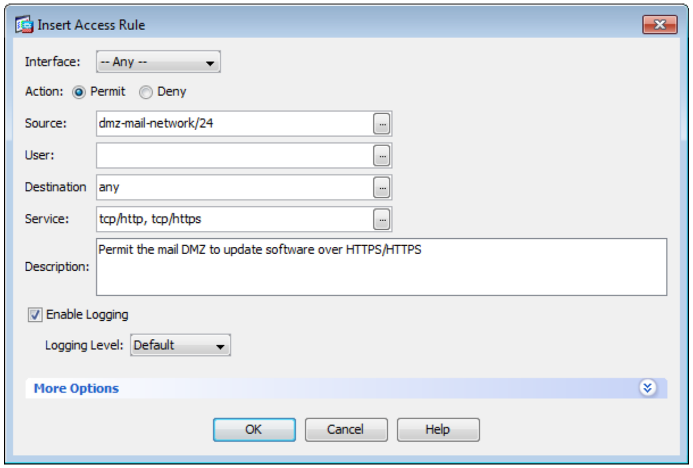
Step 40: Click **Add > Insert**.

Step 41: In the **Add Access Rule** dialog box, in the **Interface** list, select **—Any—**.

Step 42: For **Action**, select **Permit**.

Step 43: In the **Source** list, select the network object automatically created for the email DMZ. (Example: dmz-mail-network/24)

Step 44: In the **Service** list, enter **tcp/http, tcp/https**, and then click **OK**.



Interface: -- Any --

Action: ● Permit ○ Deny

Source: dmz-mail-network/24

User:

Destination: any

Service: tcp/http, tcp/https

Description: Permit the mail DMZ to update software over HTTPS/HTTPS

☑ Enable Logging

Logging Level: Default

Step 45: In the **Access Rules** window, click **Apply**.

Process

Configuring IronPort Email Security Appliance

1. Deploy IronPort ESA
2. Complete the GUI-Based System Setup
3. Install System Updates and Feature Keys

Before you begin Cisco ESA deployment, you need to configure the DNS.

The IronPort ESA host name is the name carried in the DNS MX record and indicates that the IronPort ESA is the primary MTA. The DNS A record corresponds to the IP address that Cisco Adaptive Security Appliance (ASA) is statically translating to the appliance's address in the DMZ.

Procedure 1 Deploy IronPort ESA

Step 1: To configuring management access, connect to the appliance's serial console port, using a standard null modem cable with the terminal emulator settings of 8-1-none-9600 baud.

Tech Tip

The default username is **admin**, and the default password is **ironport**.

Step 2: 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:
[]> EDIT

Enter the number of the interface you wish to edit.
[]> 1
```

```
IP interface name (Ex: “InternalNet”):
[Management]> dmz-mail

IP Address (Ex: 192.168.1.2):
[192.168.42.42]> 192.168.17.25

Ethernet interface:
1. Data 1
2. Data 2
3. Data 3
4. Management
[4]>

Netmask (Ex: “255.255.255.0” or “0xffffff00”):
[255.255.255.0]> 255.255.255.0

Hostname:
[ironport.example.com]> DMZ-ESAc370.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 Cluster Communication Service on this
interface? [N]>N
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]>

The “Demo” certificate is currently configured. You may use
“Demo”, but this will not be secure. To assure privacy, run
“certconfig” first.
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 dmz-mail 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]>
Updating SNMP agent interface referencing the old interface
name “Management” to the new interface name “dmz-mail”.
Currently configured interfaces:
1. dmz-mail (192.168.17.25/24 on Management: DMZ-ESAc370.
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.
[]>

ironport.example.com> setgateway

Enter new default gateway:[]> 192.168.17.1
```

```
ironport.example.com> commit

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

Changes committed
```

Step 3: After configuring the IronPort ESA, it should be able its default gateway.

```
ironport.example.com> ping 192.168.17.1
Press Ctrl-C to stop.
PING 192.168.17.1 (192.168.17.1): 56 data bytes
64 bytes from 192.168.17.1: icmp_seq=0 ttl=255 time=0.481 ms
64 bytes from 192.168.17.1: icmp_seq=1 ttl=255 time=0.271 ms
64 bytes from 192.168.17.1: icmp_seq=2 ttl=255 time=0.195 ms
```

Procedure 2 Complete the GUI-Based System Setup

Step 1: From a client on the internal network, navigate and login to the appliance. (Example: https://DMZ-ESAc370.cisco.local/)

Step 2: Navigate to **System Administration** > **System Setup Wizard**.

Step 3: At the **Start** screen, read the license, click **I accept**, and then click **Begin Setup**.

Step 4: On the **System** tab, in the **Default System Hostname** box, enter the appliance hostname. (Example: DMZ-ESAc370.cisco.local)

Step 5: In the **Email System Alerts** box, enter the administrators email address. (Example: admin@cisco.local)

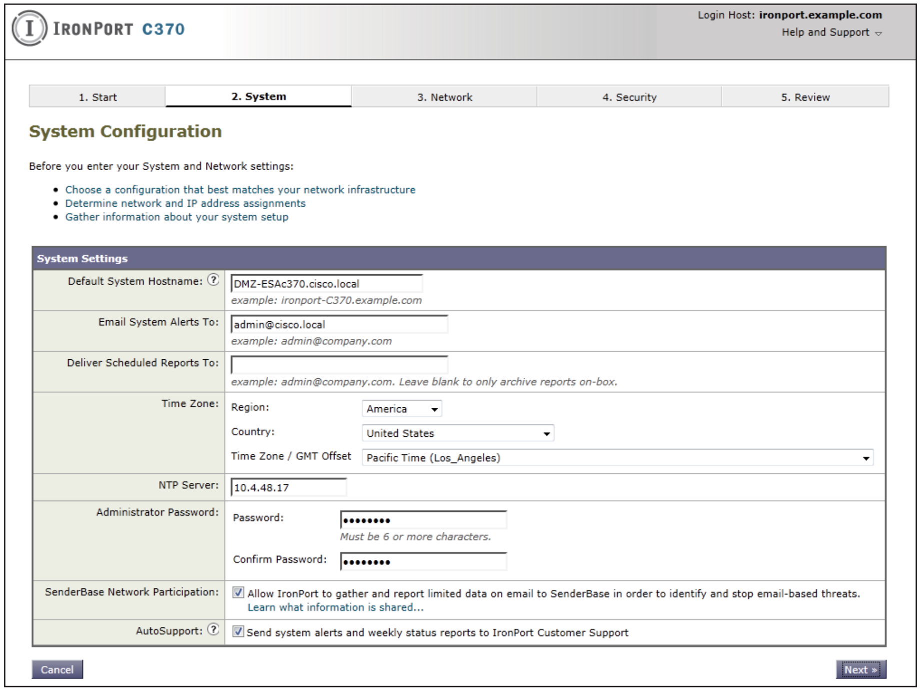
Step 6: Set the appropriate time zone for the appliance.

Step 7: In the **NTP Server** box, enter the internal NTP server. (Example: 10.4.48.17)

Step 8: Set and confirm the administrator password, and then click **Next**.

Tech Tip

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



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:	DMZ-ESAc370.cisco.local *example: ironport-C370.example.com*
Email System Alerts To:	admin@cisco.local *example: admin@company.com*
Deliver Scheduled Reports To:	*example: admin@company.com. Leave blank to only archive reports on-box.*
Time Zone:	Region: America Country: United States Time Zone / GMT Offset Pacific Time (Los_Angeles)
NTP Server:	10.4.48.17
Administrator Password:	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

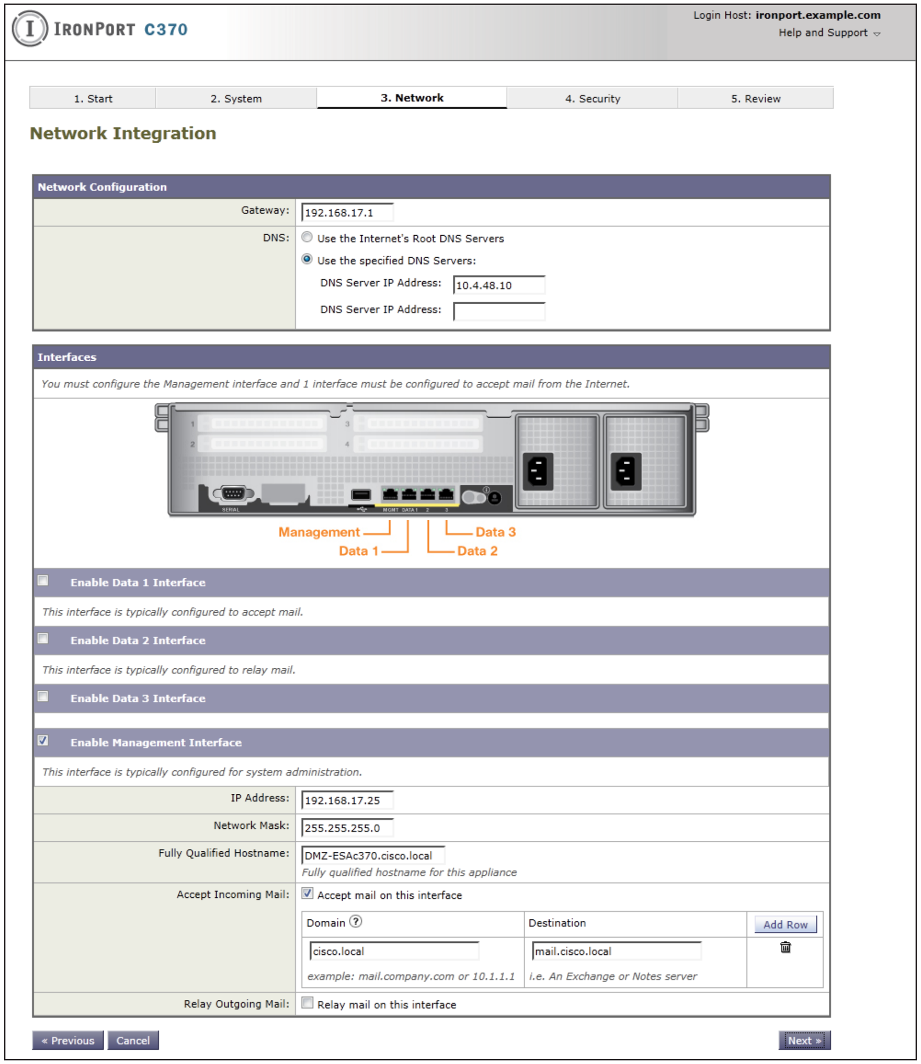
Step 9: On the **Network** tab, choose **Use the specified DNS Servers.**

Step 10: In the **DNS Server IP Address** box, enter the internal DNS. (Example: 10.4.48.10)

Step 11: Select **Accept mail on this interface**.

Step 12: In the **Domain** box, enter the organization's email domain. (Example: cisco.local)

Step 13: In the **Destination** box, enter the internal email server, and then click **Next**. (Example mail.cisco.local)



Network Integration

Network Configuration

Gateway: 192.168.17.1

DNS: ○ Use the Internet's Root DNS Servers
● Use the specified DNS Servers:
DNS Server IP Address: 10.4.48.10
DNS Server IP Address:

Interfaces

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

□ **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: 192.168.17.25

Network Mask: 255.255.255.0

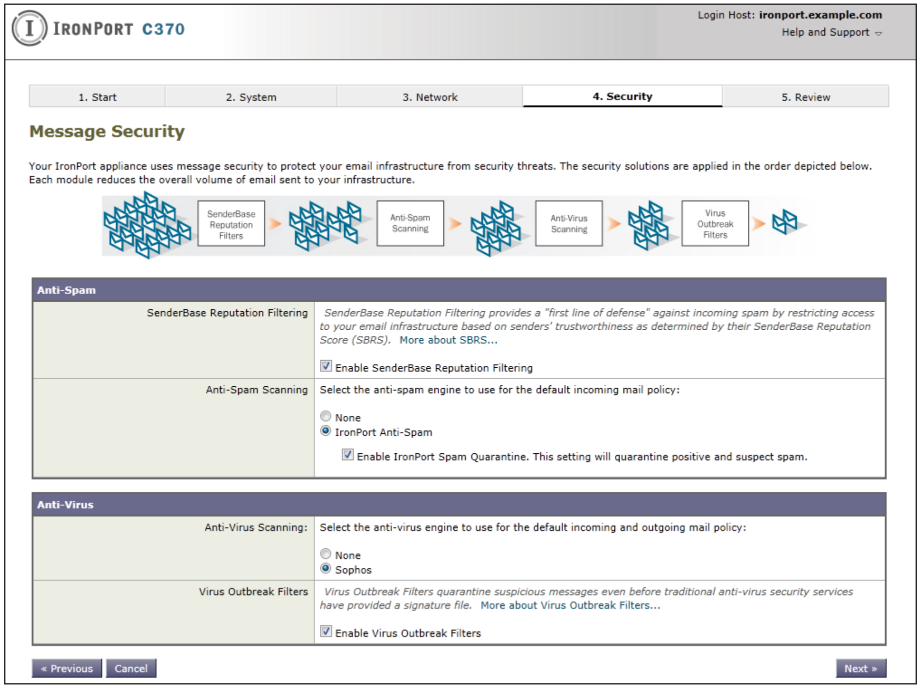
Fully Qualified Hostname: DMZ-ESAc370.cisco.local
Fully qualified hostname for this appliance

Accept Incoming Mail: ☑ Accept mail on this interface

Domain ?	Destination	Add Row
cisco.local *example: mail.company.com or 10.1.1.1*	mail.cisco.local *i.e. An Exchange or Notes server*	🗑

Relay Outgoing Mail: □ Relay mail on this interface

Step 14: On the **Security** tab, antispam and antivirus filtering are enabled by default, click **Next**.



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 (SBRS).* More about SBRS...

☑ 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
● 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 15: On the **Review** tab, review the configuration, and then click **Install this Configuration**. IronPort ESA installs the configuration.

Step 16: When the Active Directory wizard appears, click **Cancel**. In this example, you do not configure an Active Directory server.

Procedure 3 Install System Updates and Feature Keys

Step 1: In the web configuration tool, browse to **System Administration > Feature Keys**.

This is where the license keys for the different features on the box are displayed.

Step 2: Check whether your appliance has any licenses that are not currently enabled. Click the **Check for New Keys** button. This enables the appliance to connect to Cisco.com and determine if all purchased licenses are installed and enabled.

Next, you upgrade the system software on the appliance.

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.

Step 3: Select the **System Administration >System Upgrade** button. The current software version appears.

Step 4: Click **Available Updates**. This determines if updates are available.

Step 5: If newer versions are available, you may select and install them now.

Tech Tip

While it is not necessary to load all updates sequentially, it is possible that a more recent update will require interim updates before it can be loaded. If interim updates are required, the appliance will alert the operator.

Process

Enabling Mail Policies

1. Set up Bounce Verification
2. Review Incoming Mail Policies

Now that system setup is complete, you are ready to enable security services.

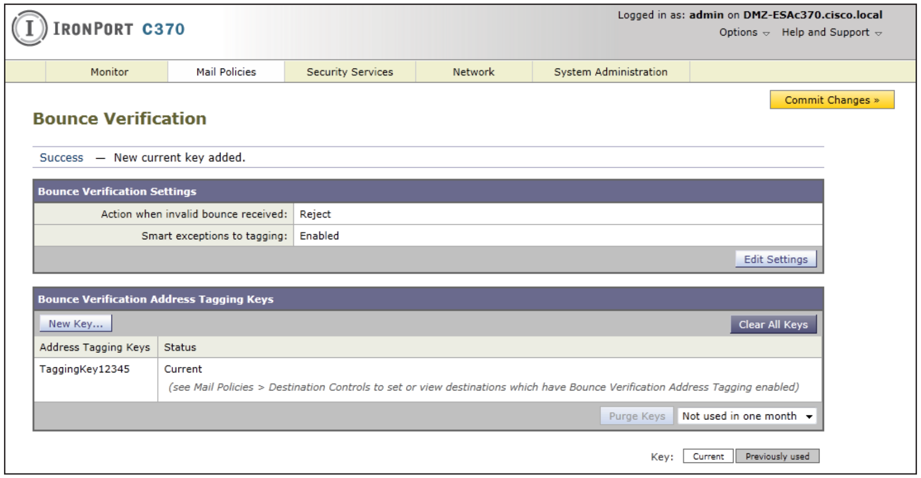
Procedure 1 Set up Bounce Verification

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

Step 1: Navigate to **Mail Policies > Bounce Verifications**, and then click **New Key.**

Step 2: In the **Address Tagging Key** box, enter an arbitrary text string that the IronPort ESA will apply in the Bounce Verification process, and then click **Submit**.

Step 3: Click **Commit Changes**.



Logged in as: admin on DMZ-ESAc370.cisco.local

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

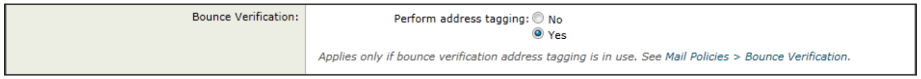
Address Tagging Keys	Status
TaggingKey12345	Current *(see Mail Policies > Destination Controls to set or view destinations which have Bounce Verification Address Tagging enabled)*

Purge Keys: Not used in one month

Step 4: Navigate to **Mail Policies > Destination Controls.**

Step 5: Under **Domain**, in the first table, click **Default**.

Step 6: Under **Bounce Verification**, change **Perform Address Tagging** to **Yes,** and then click **Submit.**



Bounce Verification: Perform address tagging: ○ No ● Yes

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

Step 7: Click **Commit Changes**.

Procedure 2 Review Incoming Mail Policies

The last stage in appliance setup is reviewing the incoming mail policies.

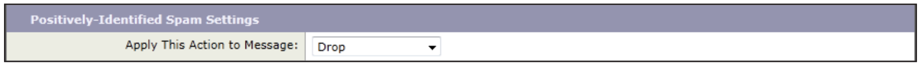
Step 1: Navigate to **Mail Policies > Incoming Mail Policies**.

Currently there is one default mail policy. It marks a positive anti-spam result for Quarantine. You will change this to instead take a Drop action.

Step 2: Under the Anti-Spam column header, select the policy definition.

Step 3: Change the **Positively-Identified Spam Settings** from **Spam Quarantine** to **Drop**, and then click **Submit**.

Step 4: Click **Commit Changes**.



Positively-Identified Spam Settings

Apply This Action to Message: Drop

Additional Information

High Availability

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

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

Monitoring

To monitor the behavior of the IronPort ESA, there are a variety of reports available under the Monitor tab. 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 IronPort 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 IronPort ESA handled the message. This search capability is especially useful if some of the more advanced features of the IronPort ESA are used, such as DLP.

Reader Tip

For more information about Cisco IronPort products, see the customer support page here:
http://www.ironport.com/support/login.html

Summary

The Cisco IronPort ESA has been configured for basic network access, and an antispam and antivirus policy has been built and applied. DNS has been modified to support the IronPort 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.

Notes

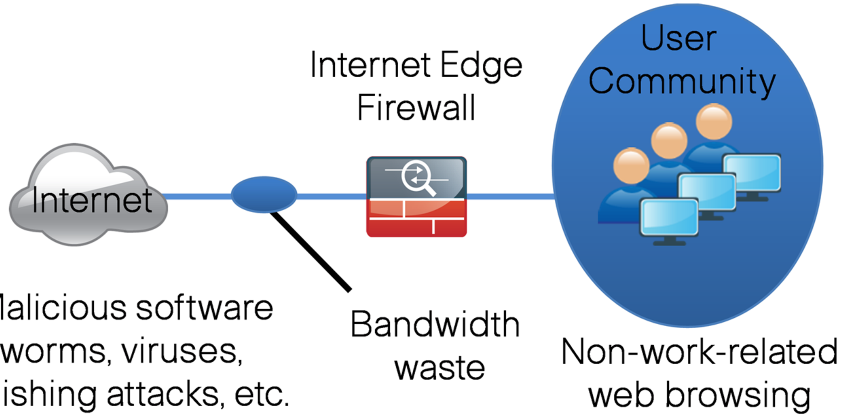
Web Security

Business Overview

Web access is a requirement for the day-to-day functions of most organizations, but a challenge exists to maintain appropriate web access for everyone in the organization, 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 organization to undue risk.

Another risk associated with Internet access for the organization 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, and 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 in the figure below.

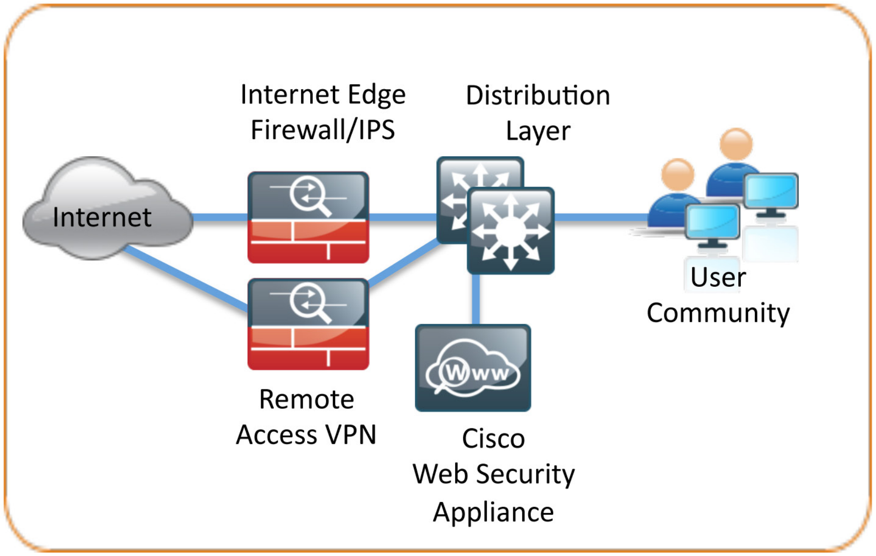
Figure 19 - Business reasons for deploying the IronPort Web Security Appliance


Internet Edge Firewall
User Community
Internet
Malicious software worms, viruses, phishing attacks, etc.
Bandwidth waste
Non-work-related web browsing

Technology Overview

Cisco IronPort S-Series Web Security Appliance (WSA) addresses the need for a corporate web security policy by offering a combination of web usage controls with category and reputation-based control, malware filtering, and data protection.

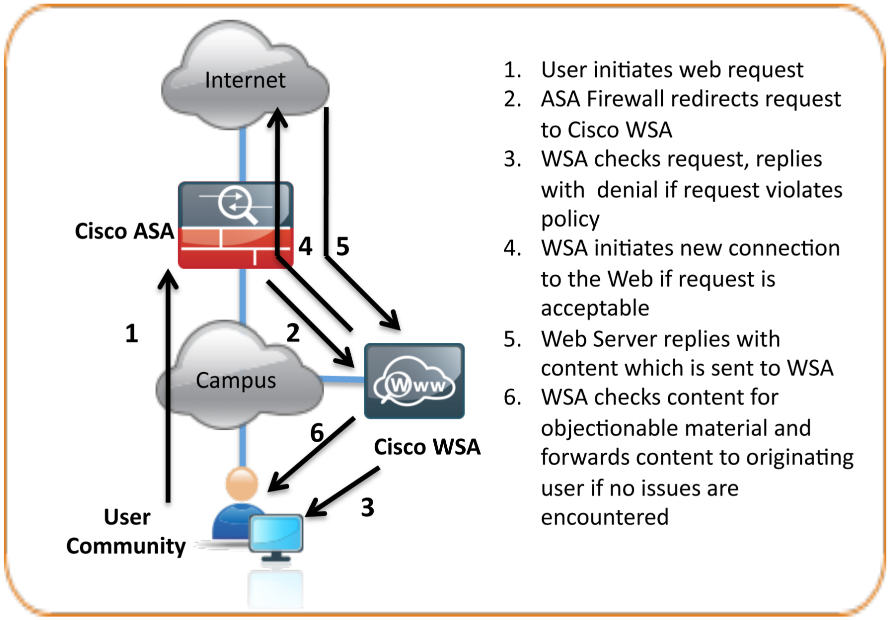
Figure 20 - Web security deployment in the borderless network



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 WSA family is a web proxy that works with other Cisco network components such as firewalls, routers or switches in order to monitor and control web content requests from within the organization. It also scrubs the return traffic for malicious content.

Figure 21 - Logical traffic flow using IronPort WSA



1. User initiates web request
2. ASA Firewall redirects request to Cisco WSA
3. WSA checks request, replies with denial if request violates policy
4. WSA initiates new connection to the Web if request is acceptable
5. Web Server replies with content which is sent to WSA
6. WSA checks content for objectionable material and forwards content to originating user if no issues are encountered

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

IronPort WSA uses several mechanisms to apply web security and content control. The IronPort WSA begins with basic URL-filtering with category-based Cisco IronPort Web Usage Controls. These controls are based on an active database that includes analysis of sites in 190 countries and 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 IronPort 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.

Deployment Details

Planning

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

In a transparent proxy deployment, a WCCP v2-capable network device redirects all TCP traffic with a destination of port 80 or 443 to the IronPort WSA, 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 IronPort WSA because all the outbound web traffic passes through the device and is generally managed by the same technicians who will manage the IronPort WSA.

An explicit proxy deployment is when a client application, such as a web browser, is configured to use an HTTP proxy, such as the IronPort 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 IronPort 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 organization with the IronPort WSA proxy settings and how they will configure devices not under the organization's control. Web Proxy Auto-Discovery and proxy automatic configuration scripts, along with other tools, such as Microsoft Group and System policy controls within Microsoft Active Directory, 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 IronPort WSA. Explicit proxy is also a good way to test the configuration of the IronPort WSA, as explicit proxy mode does not depend on anything else in the network to function.

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

Process

Configuring the IronPort WSA

1. Configure the distribution switch
2. Configure management access
3. Complete the System Setup Wizard
4. Install system updates
5. Install the feature keys
6. Enable web usage controls
7. Enable logging
8. Create custom URL categories
9. Configure access policies
10. Configure WCCP on the IronPort WSA
11. Configure WCCP on the firewall
12. Set up HTTPS proxy
13. Configure authentication

Procedure 1 Configure the distribution switch

The LAN distribution switch is the path to the organization's internal network. A unique VLAN supports the Internet Edge devices, and the routing protocol peers with the appliances across this network.

Reader Tip

This procedure assumes that the distribution switch has already been configured following the guidance in the *Smart Business Architecture—Borderless Networks for Enterprise Organizations LAN Deployment Guide*. Only the procedures required to support the integration of the firewall into the deployment are included in this guide.

Step 1: Configure the interfaces that are connected to the Internet Edge firewall.

```
interface GigabitEthernet1/0/24
 description WSAs370 M1
 switchport access vlan 300
 switchport host
```

Procedure 2 Configure management access

Step 1: To configuring management access, connect to the appliance's serial console port, using a standard null modem cable with the terminal emulator settings of 8-1-none-9600 baud.

Tech Tip

The commands that follow require a host name to be entered. This configured host name for the IronPort 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]> 10.4.24.15

Netmask (Ex: “255.255.255.0” or “0xffffff00”):
[255.255.255.0]> 255.255.255.224

Hostname:
[ironport.example.com]> WSAs370.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]>

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. Management (10.4.24.15/27 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:
[ ]> 10.4.24.1

ironport.example.com> commit

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

After configuring the IronPort 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 IronPort WSA pinging its default gateway:

```
s370.cisco.local> ping 10.4.24.1
Press Ctrl-C to stop.
PING 10.4.24.1 (10.4.24.1): 56 data bytes
64 bytes from 10.4.24.1: icmp_seq=0 ttl=255 time=0.497 ms
64 bytes from 10.4.24.1: icmp_seq=1 ttl=255 time=9.387 ms
64 bytes from 10.4.24.1: icmp_seq=2 ttl=255 time=0.491 ms
^C
```

Procedure 3 Complete the System Setup Wizard

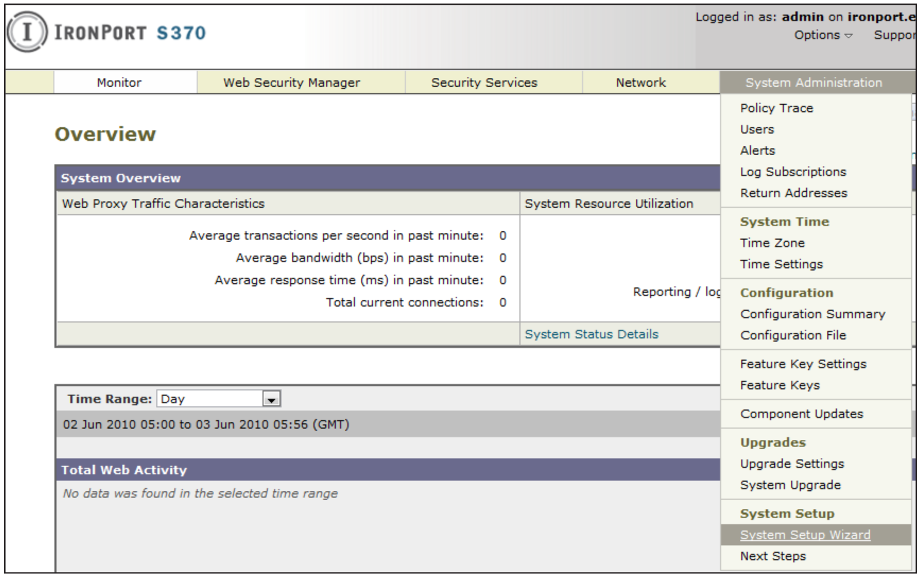
It is best to perform only the minimal configuration possible through the System Setup Wizard, leaving the more advanced configurations to their respective sections in the UI. In other words, configure only the basic network settings, DNS information, time settings, and username/password information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

Understand that the System Setup Wizard 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.

Step 1: Access the IronPort WSA GUI by opening a browser and browsing to the IP address of the IronPort WSA via HTTPS on port 8443.

```
https://wsa.cisco.local:8443
```

Step 2: Log in, and then navigate to **System Administration > System Setup Wizard**.



Overview

System Overview

Web Proxy Traffic Characteristics | System Resource Utilization

Average transactions per second in past minute:	0
Average bandwidth (bps) in past minute:	0
Average response time (ms) in past minute:	0
Total current connections:	0

Reporting / log

System Status Details

Time Range: Day

02 Jun 2010 05:00 to 03 Jun 2010 05:56 (GMT)

Total Web Activity

No data was found in the selected time range

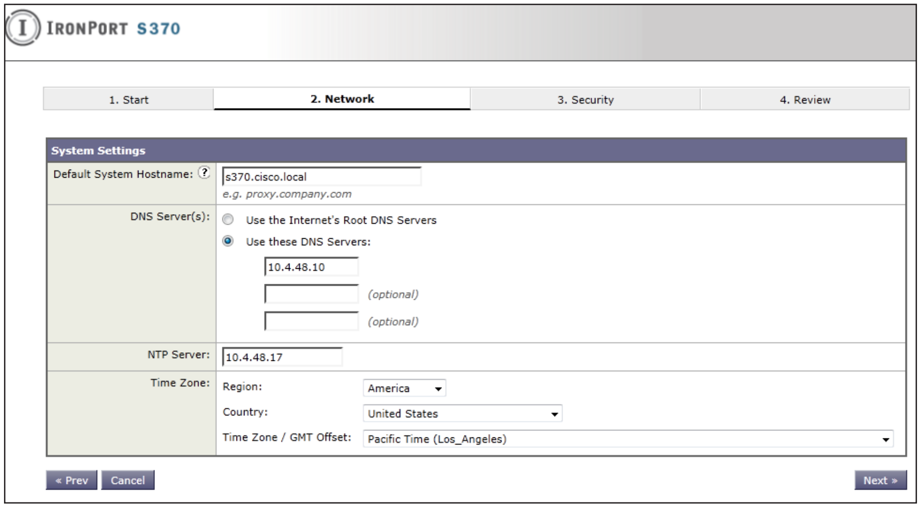
Tech Tip

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

Step 3: On the **Start** tab, read the license and accept the terms, and then click **Begin Setup**.

Step 4: Follow the instructions to complete the wizard. Note the following:

- On the **Network tab, on the System Settings** page, configure the host name, DNS server, and time settings.



System Settings

Default System Hostname: s370.cisco.local
e.g. proxy.company.com

DNS Server(s):
○ Use the Internet's Root DNS Servers
● Use these DNS Servers:
10.4.48.10
(optional)
(optional)

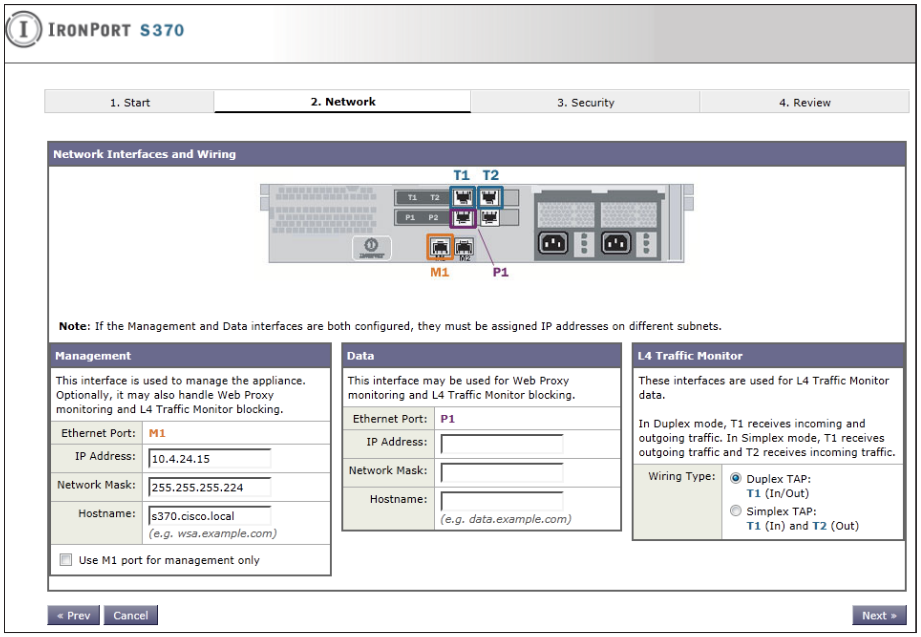
NTP Server: 10.4.48.17

Time Zone:
Region: America
Country: United States
Time Zone / GMT Offset: Pacific Time (Los_Angeles)

- On the **Network Interfaces and Wiring** page, set up which interface will be used and which IP addresses are used on each interface, and then click **Next**.

Tech Tip

In this deployment, for simplicity, M1 is used for both management and proxy services and is the only interface used. Do not select **Use M1 port for Management only.** Do not use interface P1.



Network Interfaces and Wiring

Note: If the Management and Data interfaces are both configured, they must be assigned IP addresses on different subnets.

Management

This interface is used to manage the appliance. Optionally, it may also handle Web Proxy monitoring and L4 Traffic Monitor blocking.

Ethernet Port:	M1
IP Address:	10.4.24.15
Network Mask:	255.255.255.224
Hostname:	s370.cisco.local *(e.g. wsa.example.com)*

□ Use M1 port for management only

Data

This interface may be used for Web Proxy monitoring and L4 Traffic Monitor blocking.

Ethernet Port:	P1
IP Address:	
Network Mask:	
Hostname:	*(e.g. data.example.com)*

L4 Traffic Monitor

These interfaces are used for L4 Traffic Monitor data.

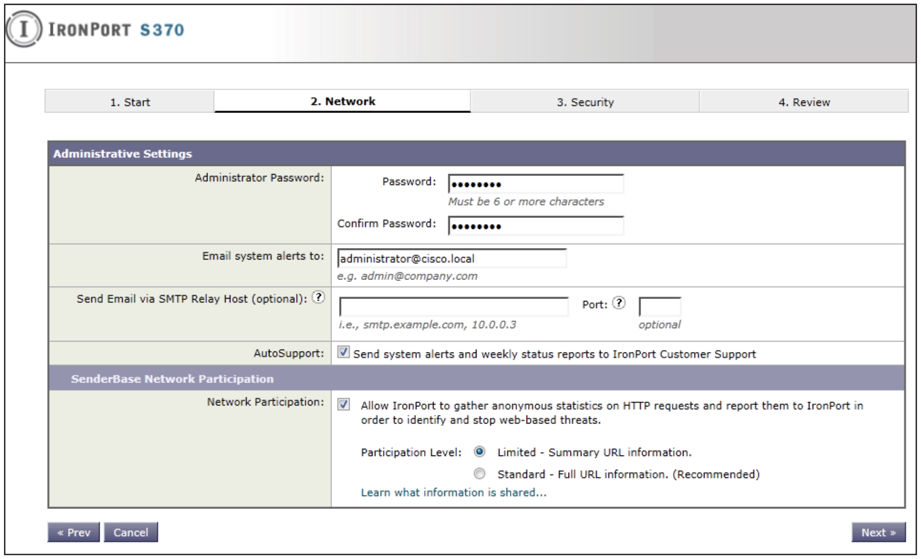
In Duplex mode, T1 receives incoming and outgoing traffic. In Simplex mode, T1 receives outgoing traffic and T2 receives incoming traffic.

Wiring Type:	● Duplex TAP: T1 (In/Out) ○ Simplex TAP: T1 (In) and T2 (Out)

- On the **Administrative Settings** page, set the admin password and the address to which system alerts will be emailed.

Tech Tip

On this page, you can also elect to participate in the SenderBase network and select a participation level.



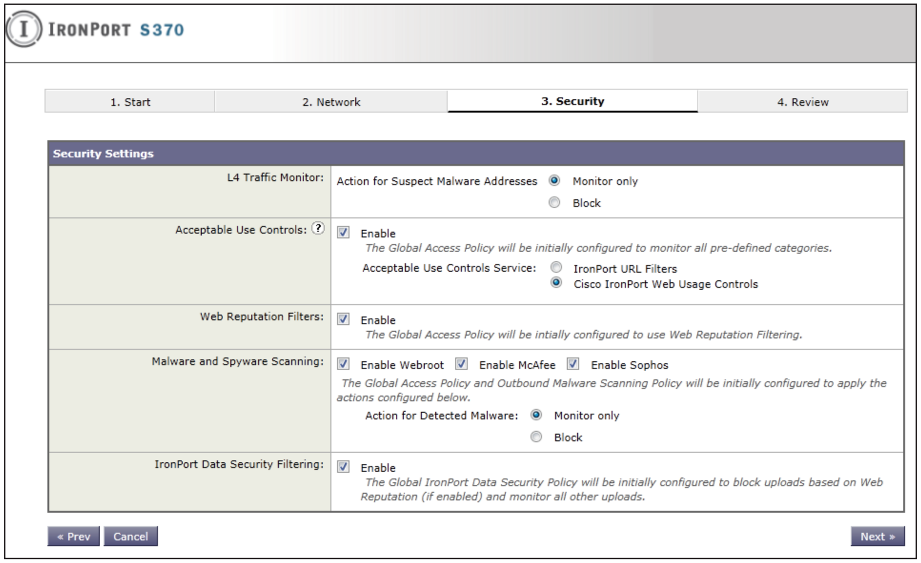
Administrative Settings

Administrator Password:	Password: •••••••• *Must be 6 or more characters* Confirm Password: ••••••••
Email system alerts to:	administrator@cisco.local *e.g. admin@company.com*
Send Email via SMTP Relay Host (optional): ?	*i.e., smtp.example.com, 10.0.0.3* Port: ? *optional*
AutoSupport:	☑ Send system alerts and weekly status reports to IronPort Customer Support

SenderBase Network Participation

Network Participation:	☑ Allow IronPort to gather anonymous statistics on HTTP requests and report them to IronPort in order to identify and stop web-based threats. Participation Level: ● Limited - Summary URL information. ○ Standard - Full URL information. (Recommended) Learn what information is shared...

- On the **Security** tab, define the security policy for the appliance and what actions will be taken for the different security features. Under **Acceptable Use Control**, select **Enable**, and then for **Acceptable Use Controls Service**, select **Cisco IronPort Web Usage Controls.**



Security Settings

L4 Traffic Monitor:	Action for Suspect Malware Addresses ● Monitor only ○ Block
Acceptable Use Controls: ?	☑ Enable *The Global Access Policy will be initially configured to monitor all pre-defined categories.* Acceptable Use Controls Service: ○ IronPort URL Filters ● Cisco IronPort Web Usage Controls
Web Reputation Filters:	☑ Enable *The Global Access Policy will be intially configured to use Web Reputation Filtering.*
Malware and Spyware Scanning:	☑ Enable Webroot ☑ Enable McAfee ☑ Enable Sophos *The Global Access Policy and Outbound Malware Scanning Policy will be initially configured to apply the actions configured below.* Action for Detected Malware: ● Monitor only ○ Block
IronPort Data Security Filtering:	☑ Enable *The Global IronPort Data Security Policy will be initially configured to block uploads based on Web Reputation (if enabled) and monitor all other uploads.*

Procedure 4 Install system updates

It is important to look at system upgrades for the IronPort WSA before going any further. HTTP or HTTPS Internet access for the IronPort WSA is required in order to proceed.

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.

Step 1: Navigate to **System Administration** > **System Upgrade**. The display will show the current software version.

Step 2: To see what updates are available, click **Available Updates**.

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

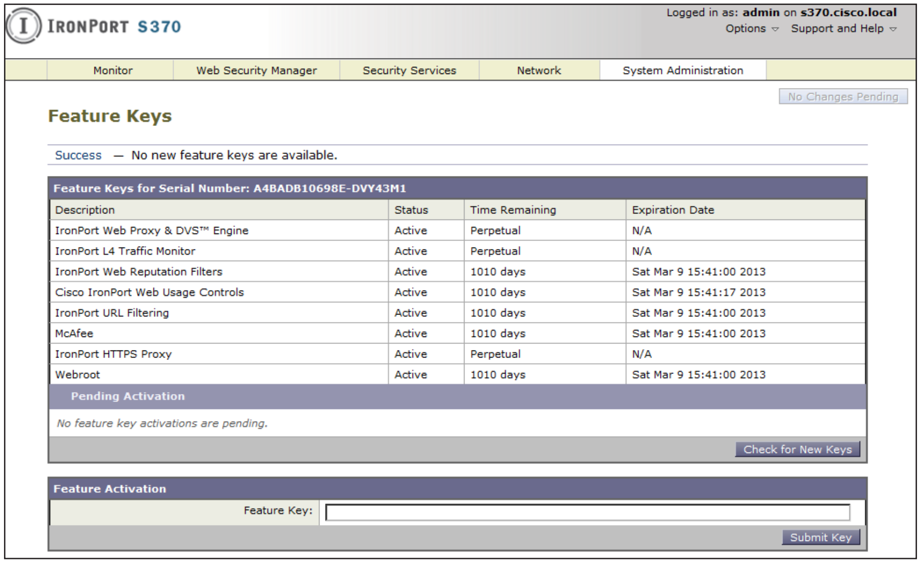
Procedure 5 Install the feature keys

It is important to install the feature keys for the IronPort WSA before going any further. HTTP or HTTPS Internet access for the IronPort WSA is required in order to proceed. When installing feature keys IronPort WSA makes 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.

Step 1: Navigate to System Administration > Feature Keys.

Step 2: To check to see whether the appliance has any licenses that are not currently enabled, click **Check for New 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.



Logged in as: admin on s370.cisco.local

Feature Keys

Success — No new feature keys are available.

Feature Keys for Serial Number: A4BADB10698E-DVY43M1

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

Pending Activation

No feature key activations are pending.

Feature Activation

Feature Key:

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.

Tech Tip

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 6 Enable web usage controls

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

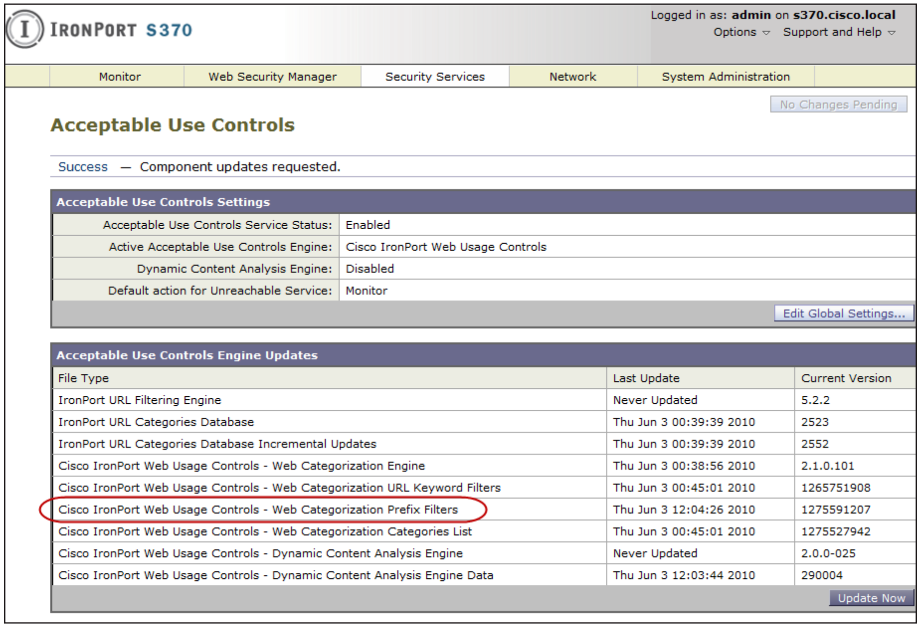
Step 1: Go to **Security Services > Acceptable Use Controls**.

Step 2: Click **Update Now,** and then wait until the page reports back success.

Step 3: Ensure that at least some of the controls have an update that is current or very nearly so.

Tech Tip

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.



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

Acceptable Use Controls Engine Updates

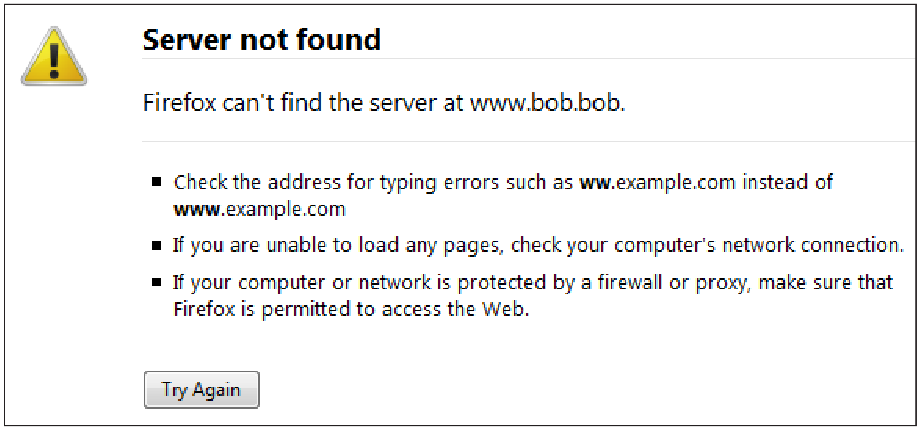
File Type	Last Update	Current Version
IronPort URL Filtering Engine	Never Updated	5.2.2
IronPort URL Categories Database	Thu Jun 3 00:39:39 2010	2523
IronPort URL Categories Database Incremental Updates	Thu Jun 3 00:39:39 2010	2552
Cisco IronPort Web Usage Controls - Web Categorization Engine	Thu Jun 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

Step 4: Set up a client on the inside of the network with the IronPort WSA as the explicit proxy in the web browser of their choice. Use the IP address of the IronPort WSA as the proxy, and then set the port to 3128.

Step 5: Test two different addresses, as follows:

- One address should be resolvable externally, for instance 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 IronPort WSA.
- The other address should be something not resolvable externally. This request should return an error from the IronPort WSA, not the browser; proving the IronPort WSA is serving the content.

Firefox returns an error like that shown below:

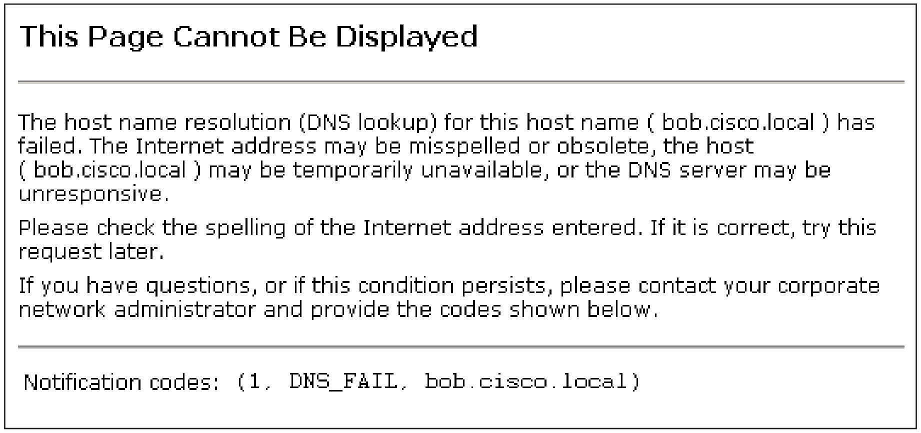


Server not found

Firefox can't find the server at www.bob.bob.

- Check the address for typing errors such as **ww**.example.com instead of **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.

The IronPort WSA returns an error like that shown below:



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)

Notes

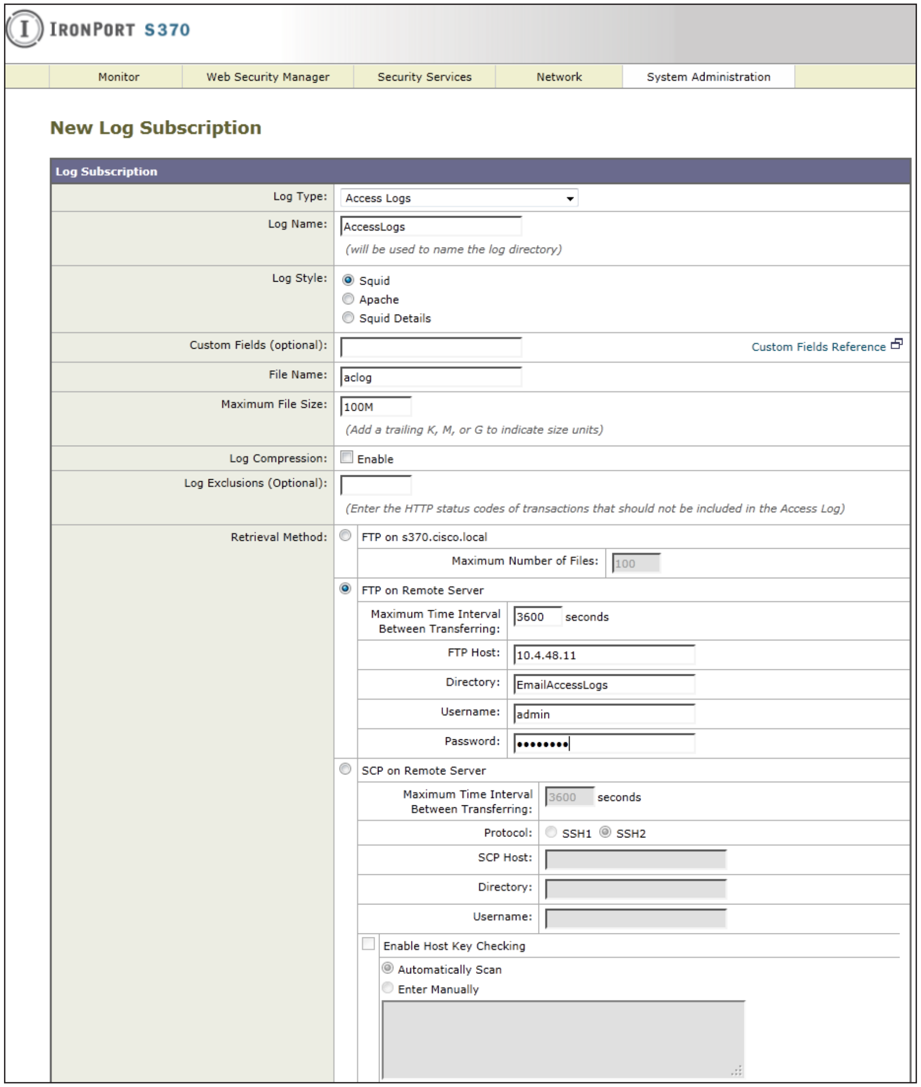
Procedure 7 Enable logging

To monitor web usage, the appliance stores client access data for a relatively short duration, and it rotates logs for space reasons. For users looking for long-term compliance reporting, they should look into the Cisco solution that comes as part of the IronPort M-Series appliance. This guide does not cover the installation or use of the IronPort M-Series appliance.

For the reporting product to work, the IronPort WSA needs to send its logs to an FTP server where the reporting device can access them. For this deployment, it is assumed an FTP server is already deployed and configured. The following configuration moves the access logs off the IronPort WSA to an FTP server.

Step 1: Navigate to **System Administration > Log Subscriptions,** and then click **Add Log Subscription.**

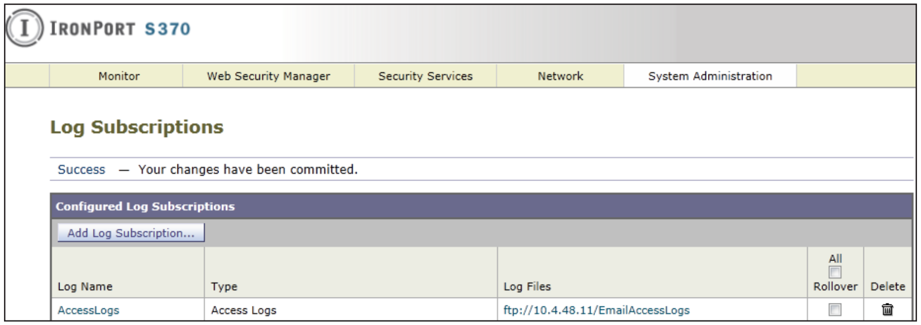
Step 2: On the **New Log Subscription** page, add the new logging information, click **Submit**, and then click **Commit Changes**.



New Log Subscription

Log Subscription	
Log Type:	Access Logs
Log Name:	AccessLogs (will be used to name the log directory)
Log Style:	● Squid ○ Apache ○ Squid Details
Custom Fields (optional):	Custom Fields Reference
File Name:	aclog
Maximum File Size:	100M (Add a trailing K, M, or G to indicate size units)
Log Compression:	□ Enable
Log Exclusions (Optional):	(Enter the HTTP status codes of transactions that should not be included in the Access Log)
Retrieval Method:	○ FTP on s370.cisco.local Maximum Number of Files: 100 ● FTP on Remote Server Maximum Time Interval Between Transferring: 3600 seconds FTP Host: 10.4.48.11 Directory: EmailAccessLogs Username: admin Password: •••••••• ○ SCP on Remote Server Maximum Time Interval Between Transferring: 3600 seconds Protocol: ○ SSH1 ● SSH2 SCP Host: Directory: Username: □ Enable Host Key Checking ● Automatically Scan ○ Enter Manually

The following figure shows the results after inputting the changes:



Log Subscriptions

Success — Your changes have been committed.

Configured Log Subscriptions

Add Log Subscription...

Log Name	Type	Log Files	All □ Rollover	Delete
AccessLogs	Access Logs	ftp://10.4.48.11/EmailAccessLogs	□	🗑

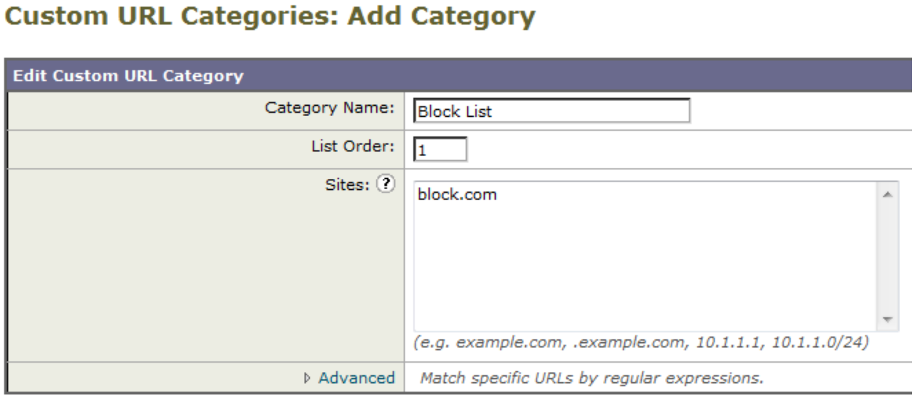
Procedure 8 Create custom URL categories

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

Step 1: Navigate to **Web Security Manager > Custom URL Categories**, and then click **Add Custom Category.**

You will create four placeholder categories for different action exceptions.

Step 2: In the **Edit Custom URL Category** pane, name the category **Block List.**



Custom URL Categories: Add Category

Edit Custom URL Category

Category Name:	Block List
List Order:	1
Sites: ?	block.com (e.g. example.com, .example.com, 10.1.1.1, 10.1.1.0/24)
▹ Advanced	Match specific URLs by regular expressions.

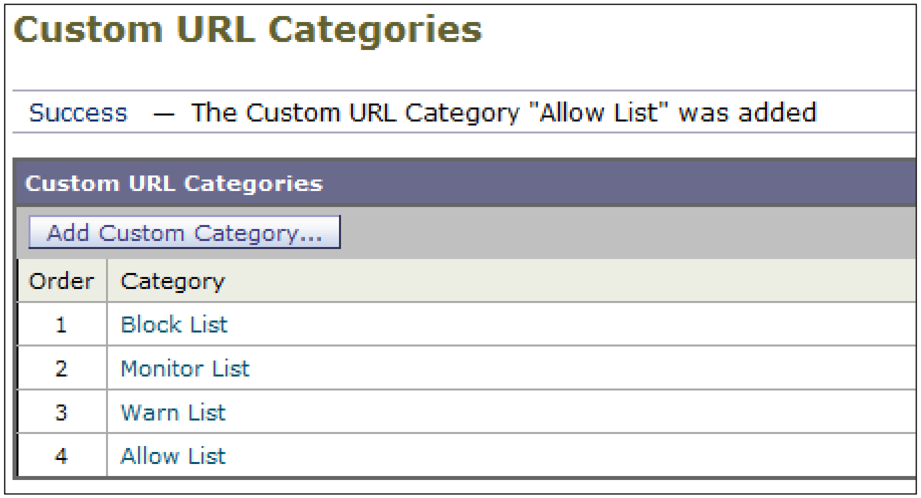
Step 3: In the **Sites** box, enter a placeholder URL (Example: block.com), and then click **Submit**.

Tech Tip

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.

Step 4: Repeat Steps 2-3, in order to create three more lists, using these three names: **Monitor List**, **Warn List,** and **Allow List** following the template above.

This will create an ordered list of custom categories.



Custom URL Categories

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

Custom URL Categories

Add Custom Category...

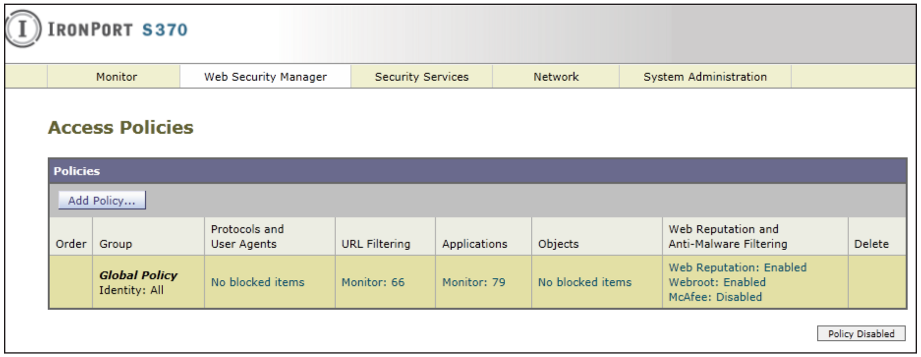
Order	Category
1	Block List
2	Monitor List
3	Warn List
4	Allow List

Step 5: Click **Commit Changes**.

Procedure 9 Configure access policies

Now that you have created the custom URL categories, you need to enable them for use and define actions for each.

Step 1: Navigate to **Web Security Manager > Access Policies,** and then under the **URL Filtering** header, click the link

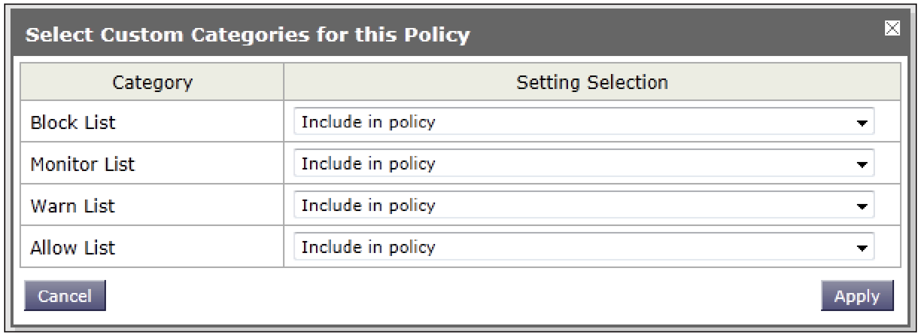


Access Policies

Policies

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Web Reputation and Anti-Malware Filtering	Delete
	Global Policy Identity: All	No blocked items	Monitor: 66	Monitor: 79	No blocked items	Web Reputation: Enabled Webroot: Enabled McAfee: Disabled	

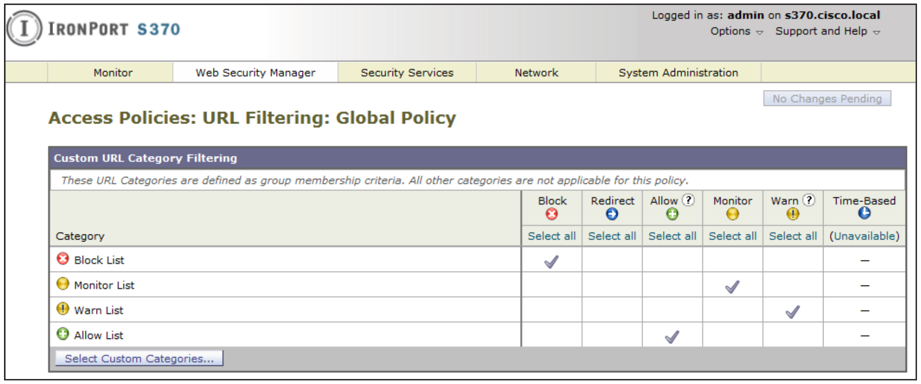
Step 2: For each custom URL category, in the **Setting Selection list, choose Include in Policy**.



Select Custom Categories for this Policy

Category	Setting Selection
Block List	Include in policy
Monitor List	Include in policy
Warn List	Include in policy
Allow List	Include in policy

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. Click **Submit.**



Logged in as: **admin** on **s370.cisco.local**

Access Policies: URL Filtering: Global Policy

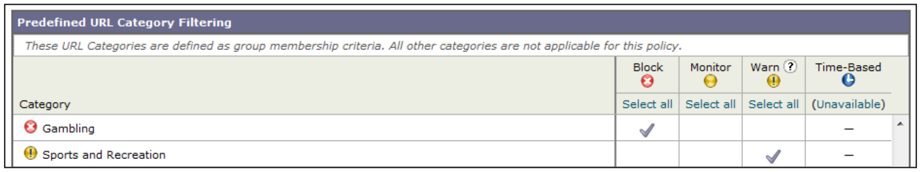
Custom URL Category Filtering

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

Category	Block	Redirect	Allow	Monitor	Warn	Time-Based
	Select all	Select all	Select all	Select all	Select all	(Unavailable)
Block List	✓					–
Monitor List				✓		–
Warn List					✓	–
Allow List			✓			–

On the **Access Policies** page, the organization'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.

Step 4: For testing purposes, change **Gambling** from **Monitor** to **Block,** change **Sports** from **Monitor** to **Warn**, and then click **Submit**.



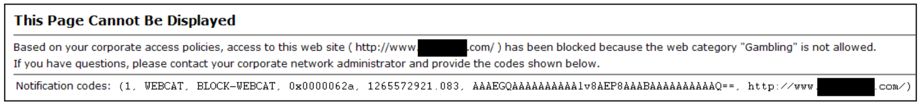
Predefined URL Category Filtering

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

Category	Block	Monitor	Warn	Time-Based
	Select all	Select all	Select all	(Unavailable)
Gambling	✓			–
Sports and Recreation			✓	–

Step 5: Using a browser explicitly pointing to the IronPort WSA appliance, try browsing to a well-known gambling site.

The IronPort WSA should return the following message.



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, AAAEGQAAAAAAAAAAlv8AEP8AAABAAAAAAAAAAQ==, http://www.[redacted].com/)
```

Procedure 10 Configure WCCP on the IronPort WSA

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

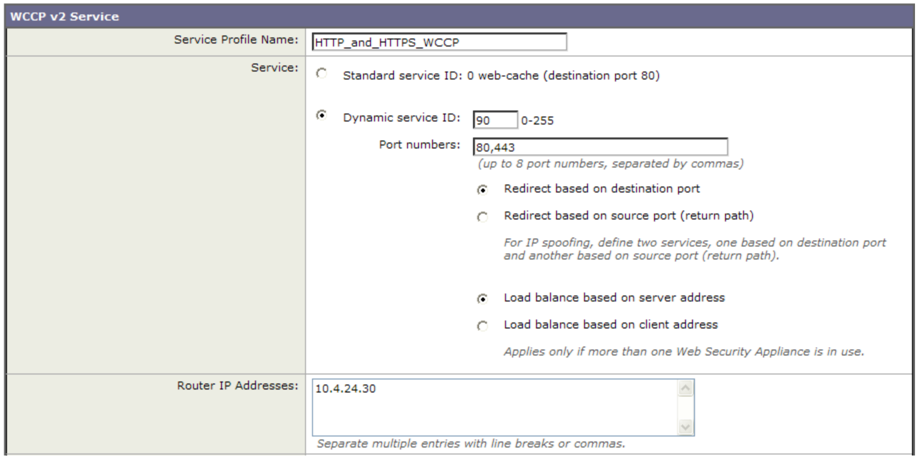
Step 1: Click **Network** > **Transparent Redirection.**

Step 2: Select **Edit Device**.

Step 3: From the **Type** list select **WCCP v2 Router**, and then click **Submit.**

Step 4: Under **WCCPv2 Services**, click **Add Service**.

Step 5: On the **WCCP v2 Service** pane, ensure the **Service Profile Name** is **HTTP_and_HTTPS_WCCP.**



WCCP v2 Service

Service Profile Name:	HTTP_and_HTTPS_WCCP
Service:	○ Standard service ID: 0 web-cache (destination port 80) ● 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 destination 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 Appliance is in use.*
Router IP Addresses:	10.4.24.30 *Separate multiple entries with line breaks or commas.*

Step 6: In the Dynamic Service ID box, enter 90. This is the number used to define this policy and is the ID used by Cisco ASA to request the policy.

Step 7: In this policy, redirect ports are HTTP and HTTPS. In the **Port numbers** box, enter **80, 443.**

Step 8: In the **Router IP Address box**, enter **10.4.24.30**. This address is inside the Cisco ASA.

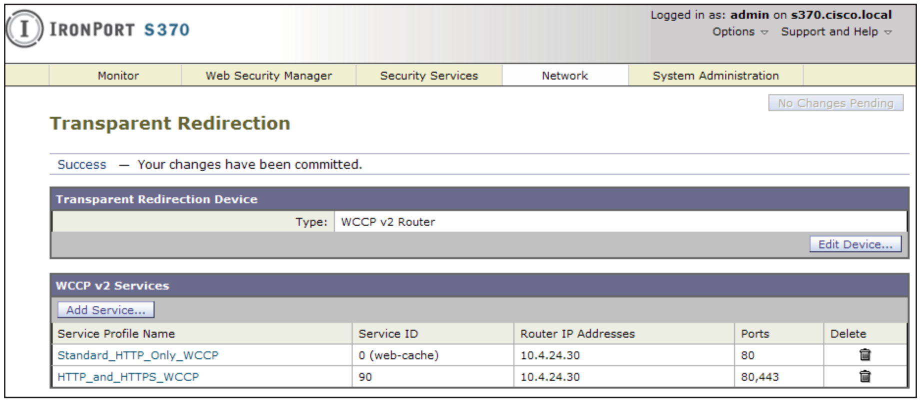
Step 9: Repeat Steps 5-8, using the following information:

- Name this policy **Standard_HTTP_Only_WCCP.**
- Select **Standard Service ID**.
- In the **Router IP Addresses** box, enter **10.4.24.30.**

Tech Tip

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

The WCCP services panel should look like the below figure after completion.



Transparent Redirection

Success — Your changes have been committed.

Transparent Redirection Device

Type: WCCP v2 Router

WCCP v2 Services

Service Profile Name	Service ID	Router IP Addresses	Ports	Delete
Standard_HTTP_Only_WCCP	0 (web-cache)	10.4.24.30	80	🗑
HTTP_and_HTTPS_WCCP	90	10.4.24.30	80,443	🗑

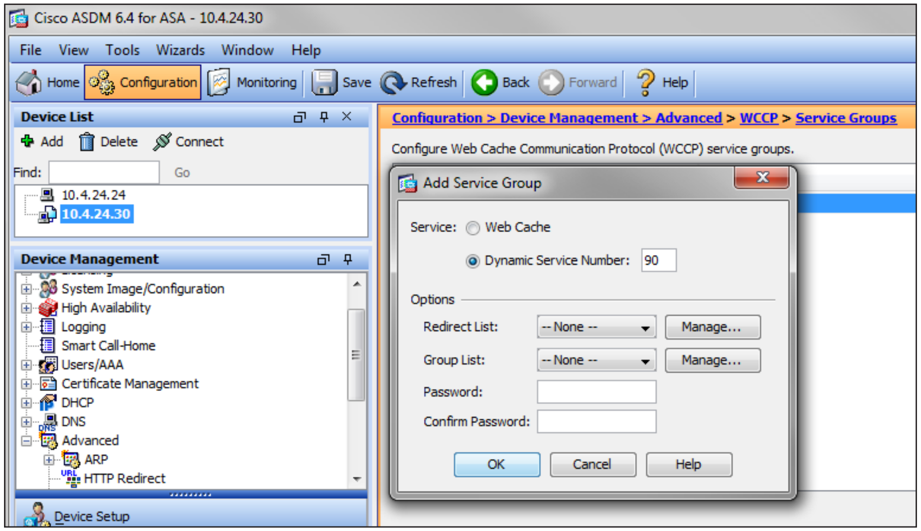
Step 10: Click **Commit Changes**.

Procedure 11 Configure WCCP on the firewall

The WCCP policy configured redirects all HTTP and HTTPS traffic to the IronPort 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 IronPort WSA. To avoid having any of this traffic redirected to the IronPort WSA, you will create an access control list (ACL) on the firewall in order to filter out any HTTP or HTTPS traffic destined to RFC 1918 addresses.

Step 1: On Cisco ASDM on the firewall, navigate to **Configuration > Device Management > Advanced > WCCP.**

Step 2: Under **Service Groups**, build a new service group using the Dynamic Service Number of 90 that you defined on the IronPort WSA.


Cisco ASDM 6.4 for ASA - 10.4.24.30
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Device List
Add Delete Connect
Find: Go
10.4.24.24
10.4.24.30
Device Management
System Image/Configuration
High Availability
Logging
Smart Call-Home
Users/AAA
Certificate Management
DHCP
DNS
Advanced
ARP
HTTP Redirect
Device Setup
Configuration > Device Management > Advanced > WCCP > Service Groups
Configure Web Cache Communication Protocol (WCCP) service groups.
Add Service Group
OK Cancel Help

Service: ○ Web Cache

● Dynamic Service Number: 90

Options

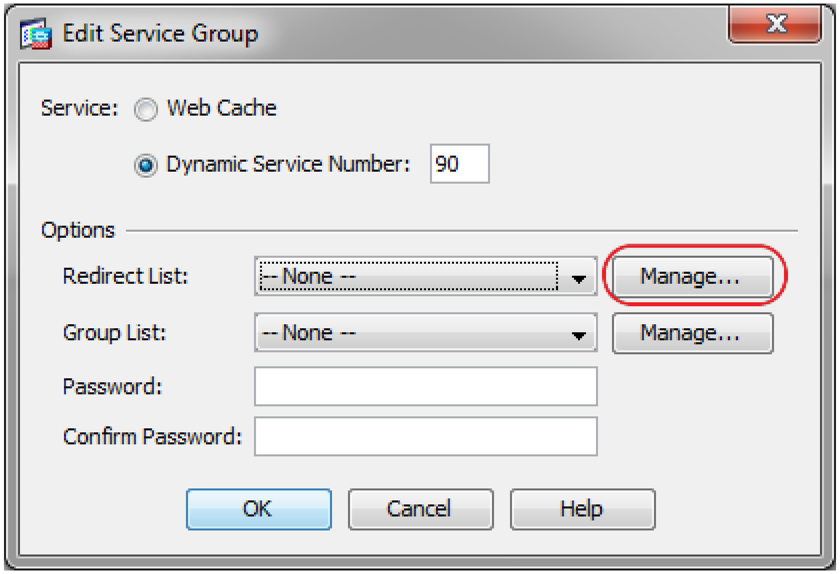
Redirect List: -- None -- Manage...

Group List: -- None -- Manage...

Password:

Confirm Password:

Step 3: In the **Add Service Groups** dialog box, next to **Redirect List**, click **Manage**.



Service: ○ Web Cache

● Dynamic Service Number: 90

Options

Redirect List: -- None -- Manage...

Group List: -- None -- Manage...

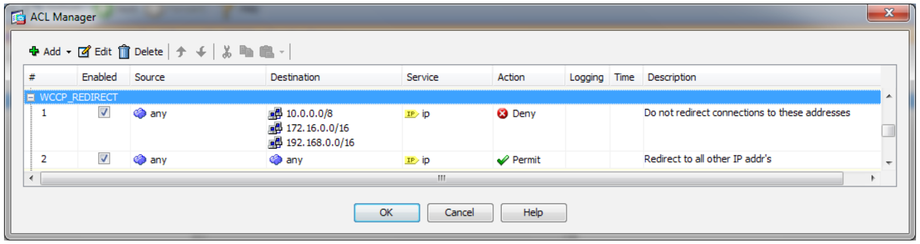
Password:

Confirm Password:

Step 4: In **ASDM > Configuration > Firewall > Advanced > ACL Manager**, click **Add**, and then select the **Add ACL** option. Input a name for the ACL: **WCCP_Redirect**

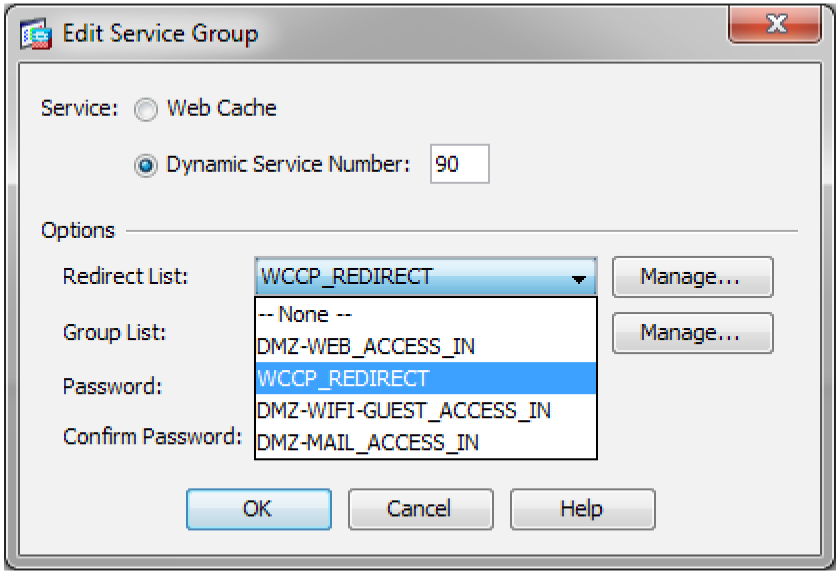
Step 5: Click **Add ACE,** and then add a line to Deny any source to all RFC 1918 addresses as the destination with a Service of IP.

Step 6: Click **Add ACE**, add a line to Permit any source to any destination with a Service of IP, and then click **OK**.



#	Enabled	Source	Destination	Service	Action	Logging	Time	Description
WCCP_REDIRECT								
1	☑	any	10.0.0.0/8 172.16.0.0/16 192.168.0.0/16	ip	Deny			Do not redirect connections to these addresses
2	☑	any	any	ip	Permit			Redirect to all other IP addr's

Step 7: On the **Edit Service Group** dialog box, in the **Redirect List drop down list, choose** the ACL created above (**WCCP_Redirect**), and then click **OK**


Edit Service Group

Service: ○ Web Cache

● Dynamic Service Number: 90

Options

Redirect List: WCCP_REDIRECT

Group List:

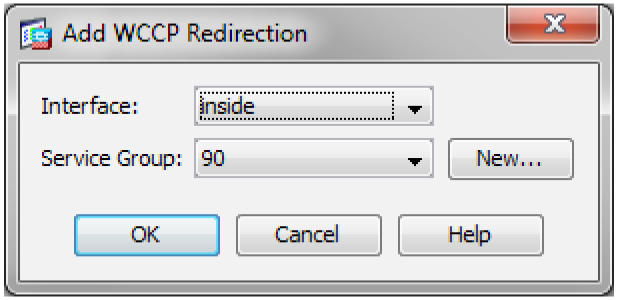
Password:

Confirm Password:

Step 8: Click **Apply**.

Step 9: Navigate to **Configuration > Device Management > Advanced > WCCP > Redirection on ASDM**, and then click **Add**.

Step 10: **In the Add WCCP Redirection dialog box, i**n the **Interface** list, choose **inside**. In the **Service Group** list, choose **90**, and then click **OK**.


Add WCCP Redirection

Interface: inside

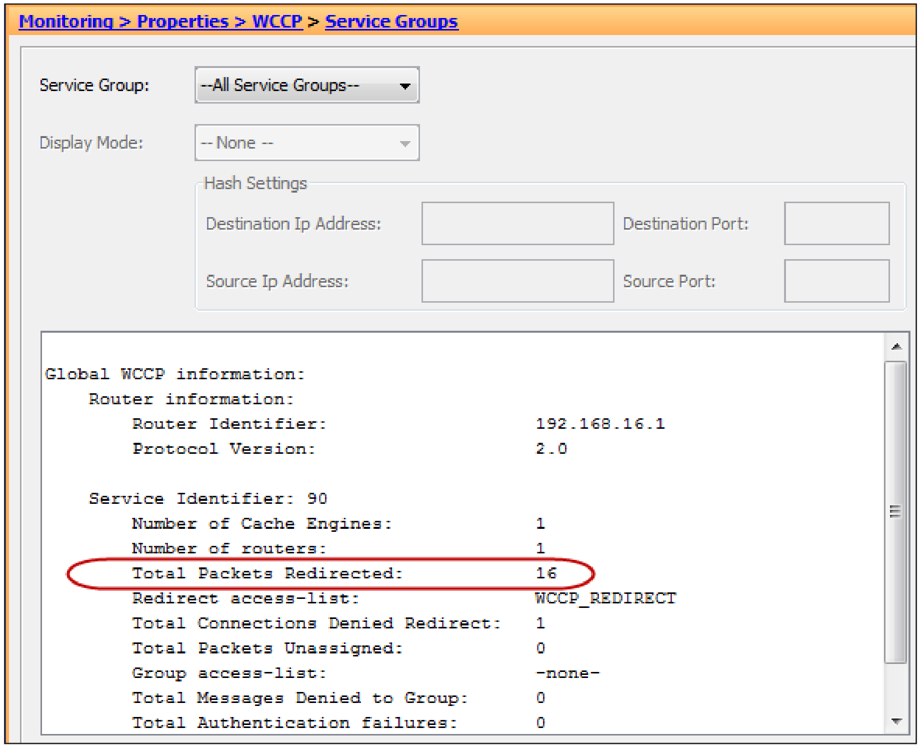
Service Group: 90

Step 11: 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), and test to the following sites:

- A resolvable allowed address such as www.cisco.com.
- A resolvable blocked address (from one of the previously configured Blocked categories)

Step 12: To check that WCCP redirection is working, in Cisco 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 appliance (in this case 192.168.16.1) and the number of cache engines is 1, which is the IronPort WSA appliance. If things are working correctly and redirections are occurring, the Total Packets Redirected counter will be increasing.


Monitoring > Properties > WCCP > Service Groups

Service Group: --All Service Groups--

Display Mode: -- None --

Hash Settings

Destination Ip Address:

Destination Port:

Source Ip Address:

Source Port:

```
Global WCCP information:
    Router information:
        Router Identifier:                    192.168.16.1
        Protocol Version:                     2.0

    Service Identifier: 90
        Number of Cache Engines:              1
        Number of routers:                    1
        Total Packets Redirected:             16
        Redirect access-list:                 WCCP_REDIRECT
        Total Connections Denied Redirect:    1
        Total Packets Unassigned:             0
        Group access-list:                    -none-
        Total Messages Denied to Group:       0
        Total Authentication failures:        0
```

High Availability and Resilience

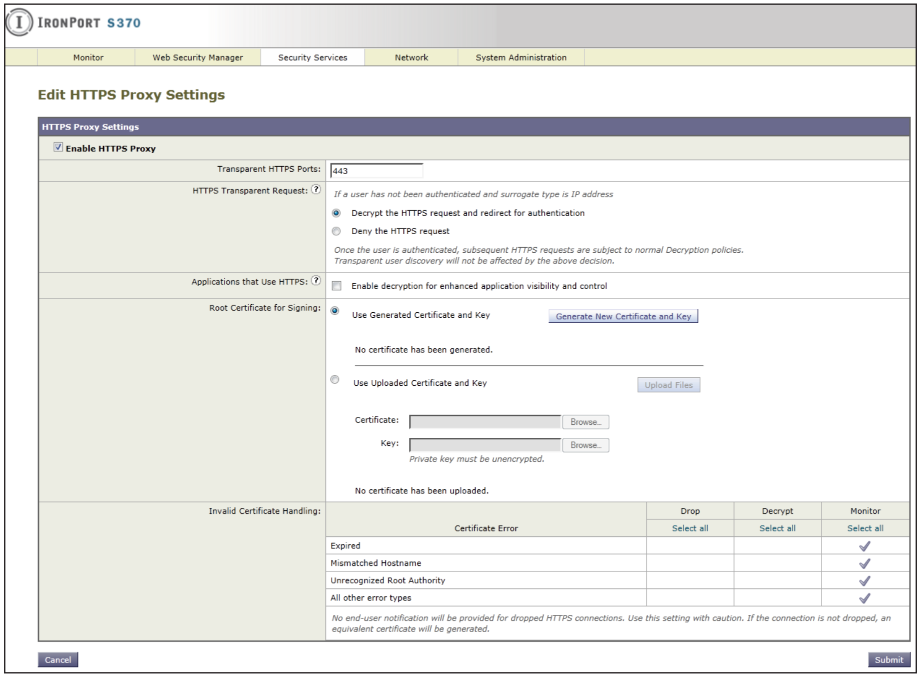
For availability purposes, if the IronPort WSA fails, the WCCP reports that fact to the appliance, and it stops redirecting traffic to the IronPort WSA by default. If web security resilience is a requirement, two or more IronPort WSAs can be deployed. To deploy multiple devices, define multiple WCCP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

Procedure 12 Set up HTTPS proxy

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

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

Step 2: On the **Edit HTTPS Proxy Settings** page, define the ports to proxy HTTPS where the default is only on TCP 443.



Edit HTTPS Proxy Settings

HTTPS Proxy Settings

☑ Enable HTTPS Proxy

Transparent HTTPS Ports: 443

HTTPS Transparent Request: *If a user has not been authenticated and surrogate type is IP address*
● Decrypt the HTTPS request and redirect for authentication
○ Deny the HTTPS request
Once the user is authenticated, subsequent HTTPS requests are subject to normal Decryption policies. Transparent user discovery will not be affected by the above decision.

Applications that Use HTTPS: □ Enable decryption for enhanced application visibility and control

Root Certificate for Signing:
● Use Generated Certificate and Key
No certificate has been generated.
○ Use Uploaded Certificate and Key
Certificate:
Key:
Private key must be unencrypted.
No certificate has been uploaded.

Invalid Certificate Handling:

Certificate Error	Drop Select all	Decrypt Select all	Monitor Select all
Expired			✓
Mismatched Hostname			✓
Unrecognized Root Authority			✓
All other error types			✓

No end-user notification will be provided for dropped HTTPS connections. Use this setting with caution. If the connection is not dropped, an equivalent certificate will be generated.

Step 3: Define the action IronPort WSA should take when it encounters an invalid certificate on the HTTPS server. The choices, depending on the certificate error, can range from dropping the connection, decrypting it, or monitoring it.

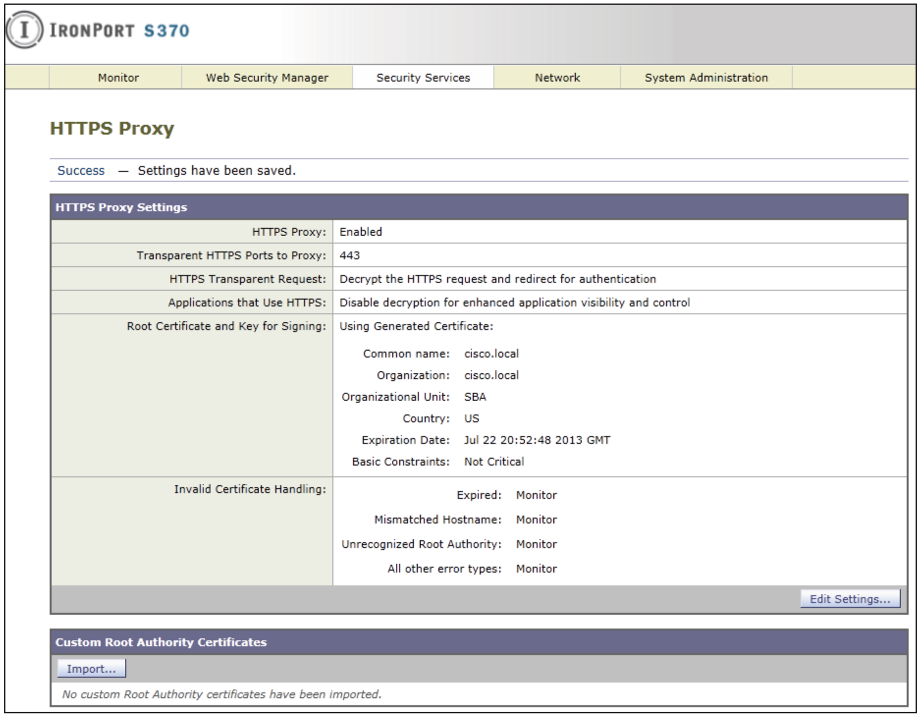
Tech Tip

You need to generate a certificate for the IronPort WSA to use on the client side of the proxy connection. 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 organization 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.

Step 4: When you are finished editing, click **Submit** and then **Commit Changes**.

Reader Tip

For more information about using certificates as part of the IronPort WSA HTTPS proxy mechanism, see the *IronPort WSA User Guide*, or consult a trusted partner or Cisco sales representative.



HTTPS Proxy

Success — Settings have been saved.

HTTPS Proxy Settings

HTTPS Proxy:	Enabled
Transparent HTTPS Ports to Proxy:	443
HTTPS Transparent Request:	Decrypt the HTTPS request and redirect for authentication
Applications that Use HTTPS:	Disable decryption for enhanced application visibility and control
Root Certificate and Key for Signing:	Using Generated Certificate: Common name: cisco.local Organization: cisco.local Organizational Unit: SBA Country: US Expiration Date: Jul 22 20:52:48 2013 GMT Basic Constraints: Not Critical
Invalid Certificate Handling:	Expired: Monitor Mismatched Hostname: Monitor Unrecognized Root Authority: Monitor All other error types: Monitor

Custom Root Authority Certificates

No custom Root Authority certificates have been imported.

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

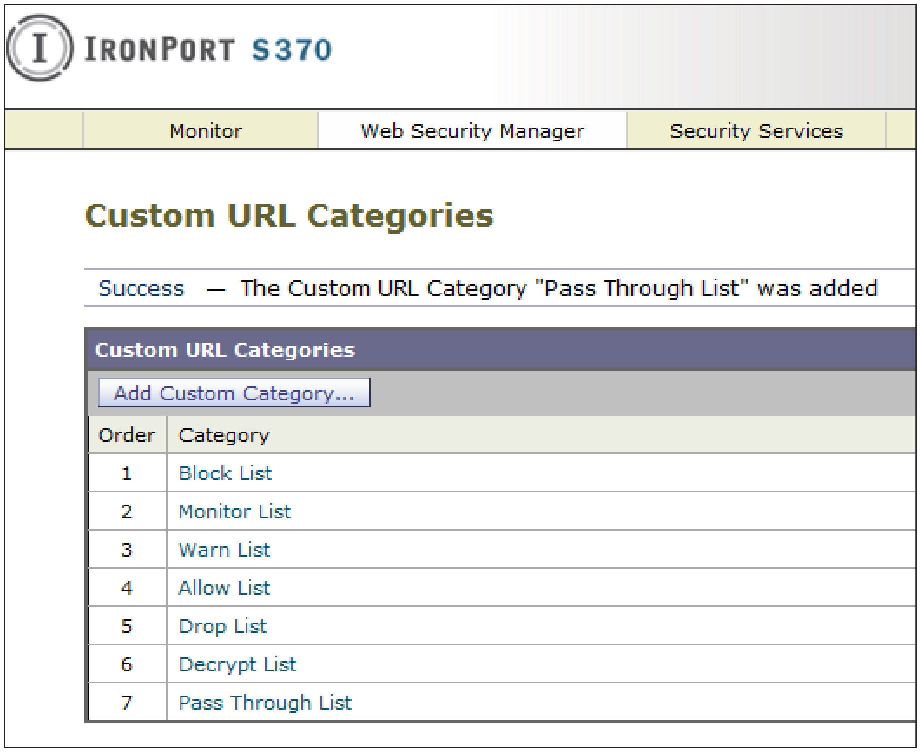
Step 5: Select Navigate to **Web Security Manager > Custom URL Categories**, and then click **Add Custom Category**.

You will create four placeholder categories for different action-exceptions.

Step 6: In the **Edit Custom URL Category** pane, name the category **Drop List.**

Step 7: In the **Sites** box, enter a placeholder URL (Example: drop.com), and then click **Submit**.

Step 8: Repeat Step 6-Step 7 to create two more custom categories, name **them Decrypt List** and **Pass Through List**, and then click **Commit Changes**.



Custom URL Categories

Success — The Custom URL Category "Pass Through List" was added

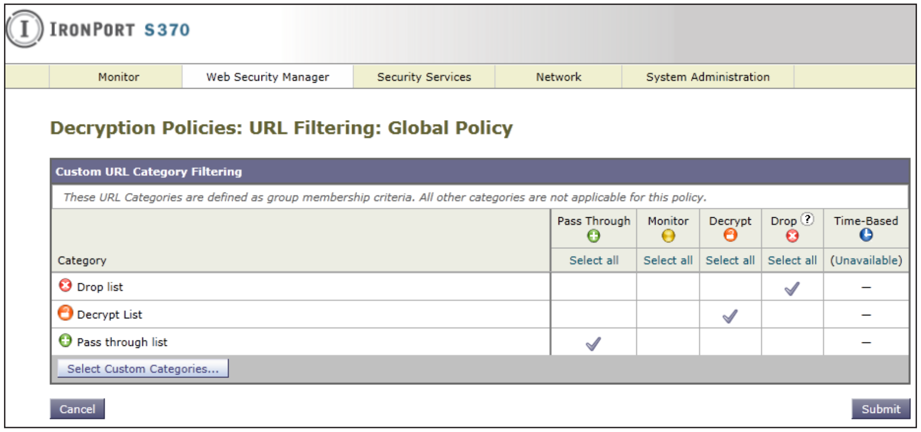
Custom URL Categories

Order	Category
1	Block List
2	Monitor List
3	Warn List
4	Allow List
5	Drop List
6	Decrypt List
7	Pass Through List

Step 9: Navigate to **Web Security Manager > Decryption Policies**.

Step 10: Under the **URL Categories** header, click the link.

Step 11: On the **Decryption Policies: URL Categories: Global Policy** page, include the three new custom categories, and then change the action of the category to correspond with its name. (Example: **Drop** should be the action for the **Drop List** category)



Decryption Policies: URL Filtering: Global Policy

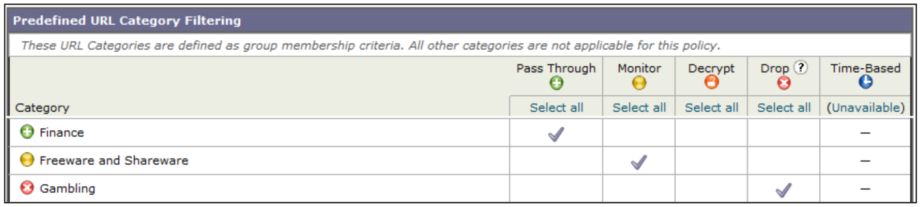
Custom URL Category Filtering

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

	Pass Through	Monitor	Decrypt	Drop	Time-Based
Category	Select all	Select all	Select all	Select all	(Unavailable)
Drop list				✓	–
Decrypt List			✓		–
Pass through list	✓				–

The predefined URL categories at the bottom of the page allow an administrator to create and enforce a policy around how the IronPort WSA handles specific types of websites with relation to decryption. Some organizations have strict policies about not decrypting health care or financial websites and potentially other categories as well. The categories on this page allow an administrator to enforce that policy on the IronPort WSA. For example, it is possible to configure the IronPort 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 12: Change the action for **Gambling** to **Drop**, and change the action for **Finance** to **Pass Through**.



Predefined URL Category Filtering

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

	Pass Through	Monitor	Decrypt	Drop	Time-Based
Category	Select all	Select all	Select all	Select all	(Unavailable)
Finance	✓				–
Freeware and Shareware		✓			–
Gambling				✓	–

Step 13: 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, use a custom URL categorie and put the address into the Drop List. When that site is accessed, the IronPort WSA should drop the connection.

Procedure 13 Configure authentication

Authentication is the act of confirming the identity of a user. When authentication is enabled, the IronPort WSA authenticates clients on the network before allowing them to connect to a destination server. When using authentication in the IronPort 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 IronPort WSA can match 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 IronPort WSA supports two different authentication protocols: lightweight directory access protocol (LDAP) and NT LAN Manager (NTLM). Because most organizations have an Active Directory server, they will be using NTLM. Single Sign-On is also only available when using NTLM.

When the IronPort WSA is deployed in transparent mode with authentication enabled and a transaction requires authentication, the IronPort WSA asks for authentication credentials from the client application. However, not all client applications support authentication, so they have no way to prompt users to provide their user names and passwords. These applications might have issues when the IronPort 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 IronPort 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)

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.

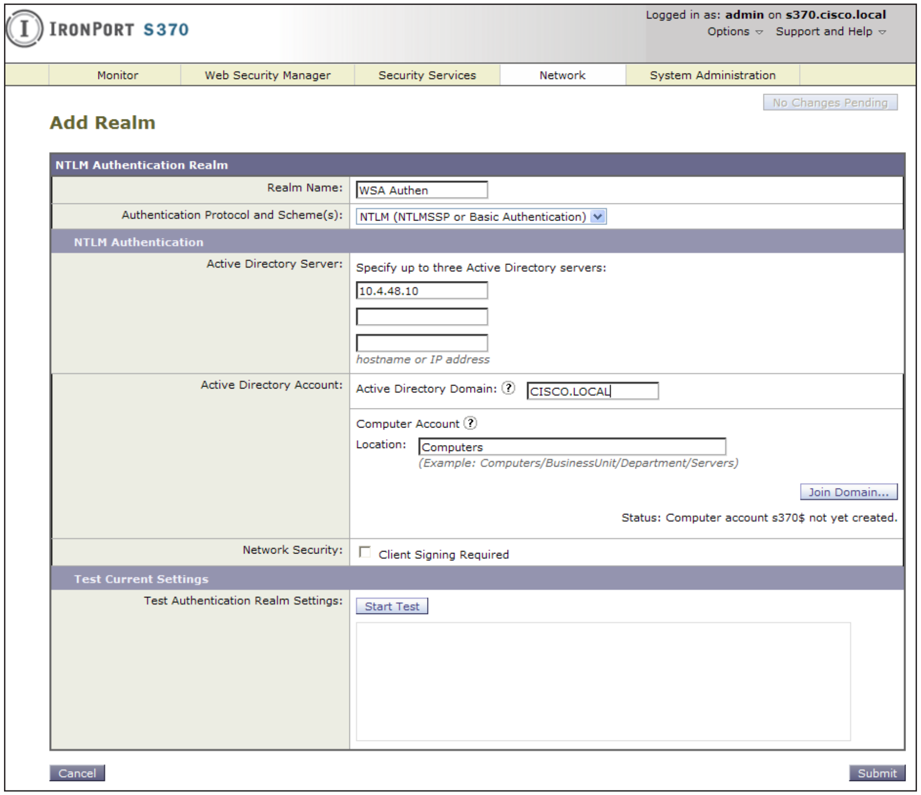
For organizations that require authentication, consult a trusted Cisco IronPort Partner or Reseller or your Cisco account team. They will be able to assist in setting up an authentication solution that meets the organization's requirements, while minimizing any possible complications.

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 Active Directory server.

Step 1: Navigate to **Network > Authentication > Add Realm**.

Step 2: On the **Add Realm** page, specify the **Active Directory Server** and the **Active Directory Domain**, and then click **Join Domain**.



Add Realm

NTLM Authentication Realm

Realm Name: WSA Authen

Authentication Protocol and Scheme(s): NTLM (NTLMSSP or Basic Authentication)

NTLM Authentication

Active Directory Server: Specify up to three Active Directory servers:
10.4.48.10
hostname or IP address

Active Directory Account: Active Directory Domain: CISCO.LOCAL

Computer Account
Location: Computers
(Example: Computers/BusinessUnit/Department/Servers)

Join Domain...

Status: Computer account s370$ not yet created.

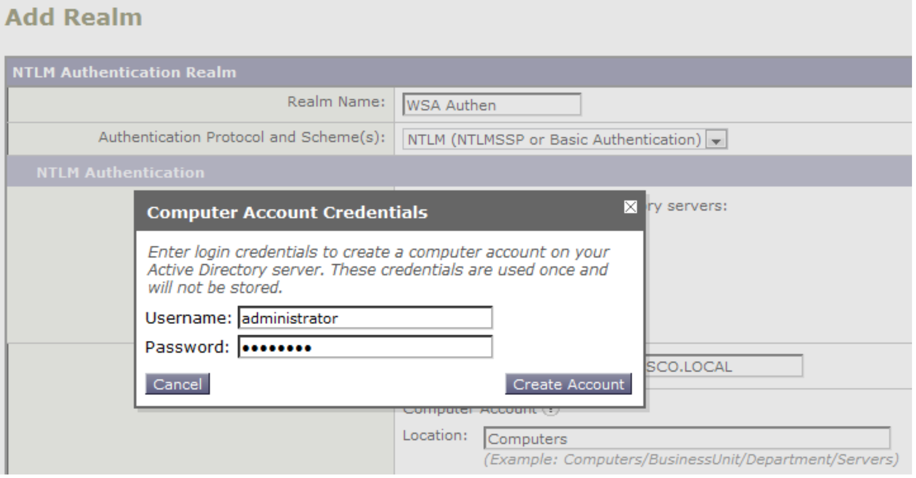
Network Security: □ Client Signing Required

Test Current Settings

Test Authentication Realm Settings: Start Test

Cancel Submit

Step 3: In the **Computer Account Credentials** dialog box, enter the Active Directory domain administrator credentials (or ask an administrator to enter them), and then click **Create Account**.


Add Realm
NTLM Authentication Realm
Realm Name: WSA Authen
Authentication Protocol and Scheme(s): NTLM (NTLMSSP or Basic Authentication)
NTLM Authentication
ry servers:
SCO.LOCAL
Computer Account
Location: Computers
(Example: Computers/BusinessUnit/Department/Servers)

Computer Account Credentials

Enter login credentials to create a computer account on your Active Directory server. These credentials are used once and will not be stored.

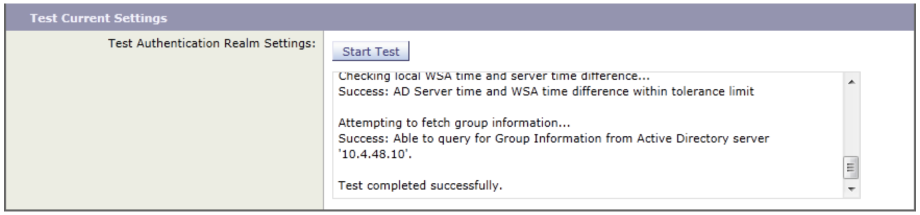
Username: administrator

Password: ••••••••

Cancel Create Account

Step 4: On the **Add Realm** page, click **Start Test**. This tests the NTLM connection to the Active Directory domain.

Step 5: If the test is successful, click **Submit** and **Commit Changes**.



Test Authentication Realm Settings:

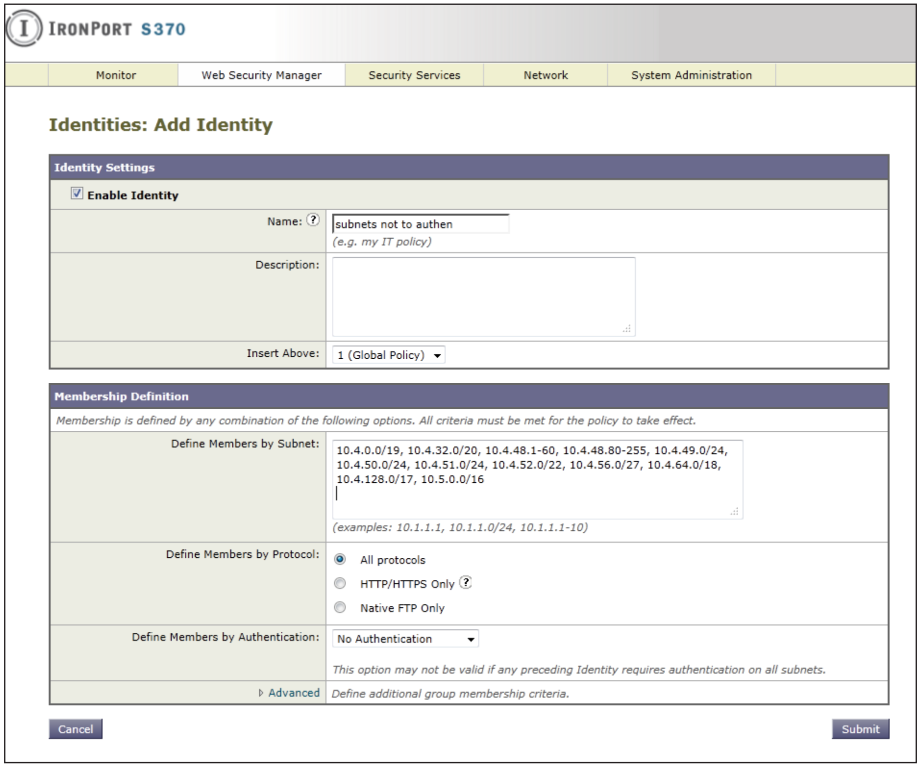
```
Checking local WSA time and server time difference...
Success: AD Server time and WSA time difference within tolerance limit

Attempting to fetch group information...
Success: Able to query for Group Information from Active Directory server
'10.4.48.10'.

Test completed successfully.
```

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

Step 6: Navigate to **Web Security Manager > Identities**, and then click **Add Identity**.

You will create two different sample identities: **Subnets not to Authen** and **User Agents not to Authen**.

Step 7: On the **Add Identity** page, in the **Name** box, enter **Subnets not to Authen**.



Identities: Add Identity

Identity Settings

☑ Enable Identity

Name: subnets not to authen
(e.g. my IT policy)

Description:

Insert Above: 1 (Global Policy)

Membership Definition

Membership is defined by any combination of the following options. All criteria must be met for the policy to take effect.

Define Members by Subnet: 10.4.0.0/19, 10.4.32.0/20, 10.4.48.1-60, 10.4.48.80-255, 10.4.49.0/24, 10.4.50.0/24, 10.4.51.0/24, 10.4.52.0/22, 10.4.56.0/27, 10.4.64.0/18, 10.4.128.0/17, 10.5.0.0/16
(examples: 10.1.1.1, 10.1.1.0/24, 10.1.1.1-10)

Define Members by Protocol:
● All protocols
○ HTTP/HTTPS Only
○ Native FTP Only

Define Members by Authentication: No Authentication
This option may not be valid if any preceding Identity requires authentication on all subnets.

Advanced: *Define additional group membership criteria.*

Step 8: In the **Define Members by Subnet** box, enter the subnet that you want to allow access to the Internet without authentication. (Example: 10.4.48.0/24)

Step 9: In the **Define Members by Authentication** list, choose **No Authentication**, and then click **Submit**.

Tech Tip

Understand that performing this action defeats the purpose of running authentication for that IP address and that log information from the IronPort 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 IronPort WSA.

Step 10: On the **Identities** page, click **Add Identity**.

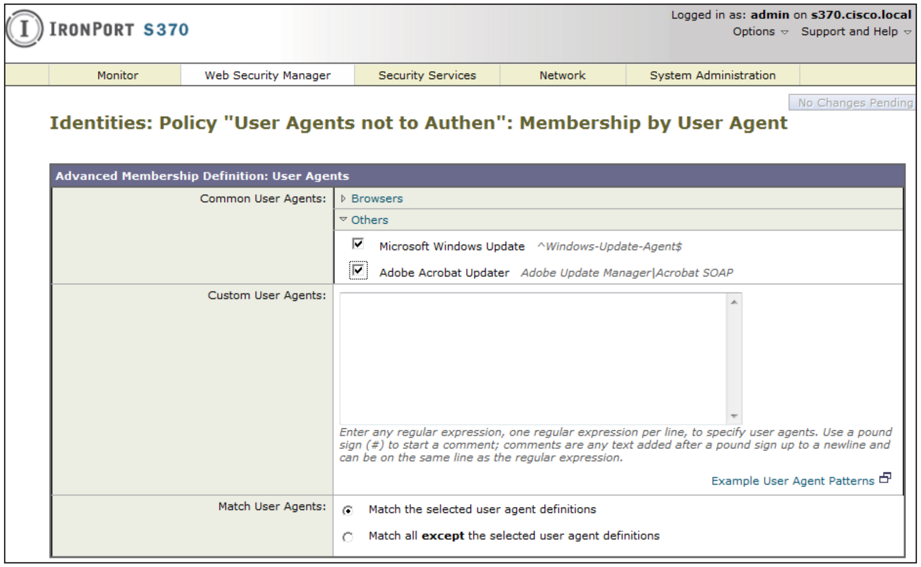
Step 11: On the **Add Identity** page, in the **Name** box, enter **User Agents not to Authen**.

Step 12: At the bottom of the page, click **Advanced**.

Step 13: On the **Membership by User Agent** page, select **Microsoft Windows Update** and **Adobe Acrobat Updater**.

Tech Tip

Selecting these agents means that when connections over HTTP with those User Agents in the HTTP Header are seen, no authentication will be requested.



Identities: Policy "User Agents not to Authen": Membership by User Agent

Advanced Membership Definition: User Agents

Common User Agents: ▷ Browsers
▽ Others
☑ Microsoft Windows Update ^Windows-Update-Agent$
☑ Adobe Acrobat Updater Adobe Update Manager|Acrobat SOAP

Custom User Agents:
Enter any regular expression, one regular expression per line, to specify user agents. Use a pound sign (#) to start a comment; comments are any text added after a pound sign up to a newline and can be on the same line as the regular expression.
Example User Agent Patterns

Match User Agents: ● Match the selected user agent definitions
○ Match all **except** the selected user agent definitions

Step 14: In the **Custom User Agents** box, enter any application that uses HTTP and is failing authentication.

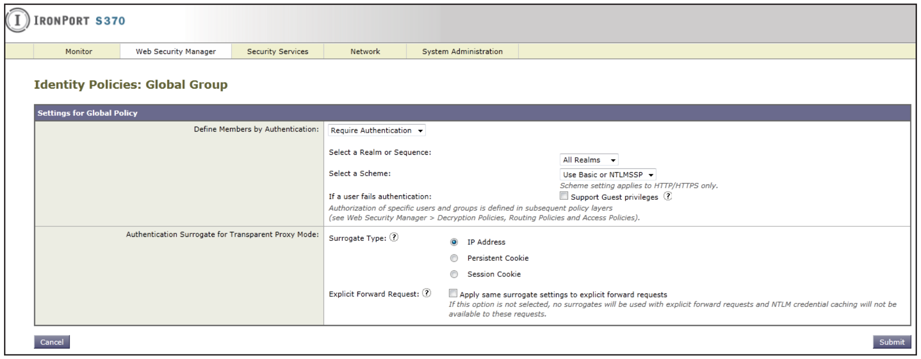
Tech Tip

If it is not possible to enter the application that is failing, then a specific custom URL category can be built and then used in the Advanced tab for URL categories.

Step 15: 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 you just built. Since those groups were built for the purpose of not authenticating, change the global identity to authenticate everybody else.

Step 16: On the **Global Group** page, in the **Define Members by Authentication** list, choose **Require Authentication**.



Identity Policies: Global Group

Settings for Global Policy

Define Members by Authentication: Require Authentication
Select a Realm or Sequence: All Realms
Select a Scheme: Use Basic or NTLMSSP
Scheme setting applies to HTTP/HTTPS only.
If a user fails authentication: ☐ Support Guest privileges
Authorization of specific users and groups is defined in subsequent policy layers (see Web Security Manager > Decryption Policies, Routing Policies and Access Policies).

Authentication Surrogate for Transparent Proxy Mode:
Surrogate Type: ● IP Address ○ Persistent Cookie ○ Session Cookie
Explicit Forward Request: ☐ Apply same surrogate settings to explicit forward requests
If this option is not selected, no surrogates will be used with explicit forward requests and NTLM credential caching will not be available to these requests.

Step 17: In the **Select a Realm or Sequence** list, choose **All Realms**.

Step 18: In the **Select a Scheme** list, choose **Basic or NTLMSSP**, and then click **Submit**.

Step 19: Click **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 is logging meets all your needs or requirements.

Internet Edge 10K Deployment

A single Cisco IronPort WSA 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 IronPort WSA S370 appliance. When deployed as above in the High Availability section, the two appliances load-share the outgoing connections. If one device fails, the load will be moved to the other IronPort 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.

Additional Information

Monitoring

To monitor the health of the IronPort WSA and the actions being taken by the IronPort WSA on traffic it is examining, there are a variety of reports available under the Monitor tab. 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 use the IronPort M-Series appliance to allow for long-term storage and reporting of events from the IronPort WSA.

Consult with your Cisco account team or your trusted partner for more information on the IronPort M-Series appliance and long-term reporting.

Troubleshooting

To determine why the IronPort 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 IronPort WSA would be if the URL were processed by the IronPort WSA. This information is especially useful if some of the more advanced features are used.

Summary

You have now installed the Cisco IronPort Web Security Appliance. A basic configuration has been applied, and the device can be inserted into the network and receive redirects from the appliance firewall. A default policy has been built that allows an organization 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 IronPort 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.

Reader Tip

For additional IronPort WSA user documentation, see the documentation here:
http://www.ironport.com/support/login.html

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

Internet Edge Server Load Balancing

Business Overview

An organization's presence on the Internet plays a key role in the success of a business. At a minimum web presence, a site that presents basic information about the organization 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 any time. 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 in order 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 Cisco Application Control Engine (ACE) is the latest SLB offering from Cisco. From its mainstream role in providing Layer 4 through 7 switching, Cisco 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 organization 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:

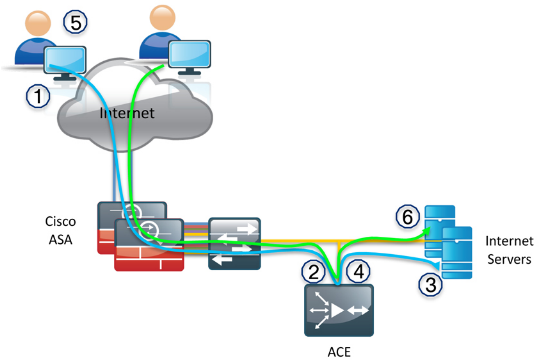
- Scalability—Cisco ACE scales the performance of a server-based application, such as a web server, by distributing its client requests across multiple servers, known as a server farm. As traffic increases, additional servers can be added to the farm.
- High Availability—Cisco ACE provides High Availability 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—Cisco 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—Cisco ACE offloads TCP and SSL processing, which allows servers to serve more users and handle more requests without increasing the number of servers.

Cisco ACE hardware is always deployed in pairs for High Availability: one primary and one secondary. If the primary Cisco ACE fails, the secondary Cisco 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 Cisco 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 Cisco ACE appliance can be deployed in several ways. "One-armed" mode is the simplest deployment method. In this mode, the Cisco ACE resides on the same VLAN as the real servers. It is not directly in the path of traffic flow and receives only traffic that is specifically intended for it. Traffic is directed to the Cisco ACE and is controlled by the design of VLANs, virtual server addresses, and server default gateway selection.

Figure 22 - Cisco ACE



1. Client starts a connection to company server
2. ACE chooses a server to assign the connection too and initiates a connection to the server
3. Connection is established to server and return traffic is sent to ACE
4. ACE connects the client and server sessions together and forwards the traffic on to the client
5. Client receives response and continues connection
6. Subsequent connections are balanced to available servers

Deployment Details

In this configuration example, you first configure the Cisco 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 Cisco ACE for the first time, but both parts can be configured via the Cisco ACE GUI. Because the example load-balancing configuration is simple, the setup in the deployment guide is shown using CLI commands.

Process

Configuring Cisco ACE Server Load Balancing

1. Setup the switch
2. Completing initial setup
3. Configure load balancing

Procedure 1 Setup the switch

Step 1: Set the DMZ switch to be the spanning tree root for the management VLAN.

```
vlan 1124
spanning-tree vlan 1124 root primary
```

Step 2: Configure the interfaces that connect to the appliances.

```
interface GigabitEthernet1/0/3
 description DMZ-ACS4710a gigabitEthernet 1/1
!
interface GigabitEthernet2/0/3
 description DMZ-ACS4710a gigabitEthernet 1/2
!
interface GigabitEthernet1/0/4
 description DMZ-ACS4710b gigabitEthernet 1/1
!
interface GigabitEthernet2/0/4
 description DMZ-ACS4710b gigabitEthernet 1/2
!
```

```
interface range GigabitEthernet1/0/3, GigabitEthernet2/0/3
  switchport
  macro apply EgressQoS
  channel-group 10 mode on
  logging event link-status
  logging event trunk-status
  logging event bundle-status
!
interface port-channel 10
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1116,1123,1124
  switchport mode trunk
  logging event link-status
  no shutdown
!
interface range GigabitEthernet1/0/4, GigabitEthernet2/0/4
  switchport
  macro apply EgressQoS
  channel-group 11 mode on
  logging event link-status
  logging event trunk-status
  logging event bundle-status
!
interface port-channel 11
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1116,1123,1124
  switchport mode trunk
  logging event link-status
  no shutdown
```

Procedure 2 Completing initial setup

Step 1: Set the system password.

When you set up the Cisco 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.
ACE>
Would you like to enter the basic configuration dialog (yes/
no) [y]: N
switch/Admin#
```

Step 2: Connect the Cisco ACE appliances.

Two Gigabit Ethernet ports on each Cisco ACE need to be configured to trunk to the switch.

```
interface gigabitEthernet 1/1
 channel-group 1
 no shutdown
interface gigabitEthernet 1/2
 channel-group 1
 no shutdown
interface port-channel 1
 port-channel load-balance src-dst-ip
 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 Cisco ACE appliances are configured for active/standby High Availability. When Cisco 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 Cisco ACE pair in order 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 3: Set up High Availability on the primary appliance.

```
interface port-channel 1
 ft-port vlan 1124
ft interface vlan 1124
  ip address 192.168.24.1 255.255.255.0
  peer ip address 192.168.24.2 255.255.255.0
  no shutdown
ft peer 1
  heartbeat interval 300
  heartbeat count 10
  ft-interface vlan 1124
ft group 1
  peer 1
  priority 120
  peer priority 110
  associate-context Admin
  inservice
```

Step 4: Set up High Availability on the secondary appliance.

```
interface port-channel 1
 ft-port vlan 1124
 no shutdown
ft interface vlan 1124
  ip address 192.168.24.2 255.255.255.0
  peer ip address 192.168.24.1 255.255.255.0
  no shutdown
ft peer 1
  heartbeat interval 300
  heartbeat count 10
  ft-interface vlan 1124
ft group 1
  peer 1
  associate-context Admin
  inservice
```

Step 5: Configure a host name

```
hostname DMZ-ACE4710a
peer hostname DMZ-ACE4710b
```

Step 6: Configure a basic access policy.

Before proceeding with additional configuration, you must set up basic network security policies in order to allow for management access into the Cisco ACE.

```
access-list ALL line 8 extended permit ip any any
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 port-channel 1
  switchport trunk allowed vlan 1116,1123
interface vlan 1123
  ip address 192.168.23.10 255.255.255.0
  peer ip address 192.168.23.11 255.255.255.0
  access-group input ALL
  service-policy input remote_mgmt_allow_policy
  no shutdown
ip route 0.0.0.0 0.0.0.0 192.168.23.1
ssh key rsa 1024 force
```

Step 7: Set up AAA.

```
tacacs-server host 10.4.48.15 key SecretKey
aaa group server tacacs+ tacacs+
  server 10.4.48.15
aaa authentication login default group tacacs+ local
```

Step 8: Configure NTP

```
ntp server 10.4.48.17
clock timezone PST -8 0
```

At this point, the Cisco ACE should be reachable on the network. Now you can begin configuring a load-balancing policy.

Step 9: Configure SNMP

```
snmp-server community cisco RO
```

Procedure 3 Configure load balancing

Step 1: Create a DMZ context.

```
context dmz-web
 allocate-interface vlan 1116
```

Step 2: Set up High Availability for the context.

```
ft group 2
  peer 1
  priority 120
  peer priority 110
  associate-context dmz-web
  inservice
```

Step 3: Change the context.

```
changeto dmz-web
```

Step 4: Create a VLAN interface and assign an IP address to it. Because you are employing one-armed mode, you need to create a NAT pool as well.

```
access-list ALL line 8 extended permit ip any any
interface vlan 1116
 ip address 192.168.16.22 255.255.255.0
 peer ip address 192.168.16.21 255.255.255.0
 access-group input ALL
 nat-pool 1 192.168.16.99 192.168.16.99 netmask 255.255.255.0
pat
 no shutdown
ip route 0.0.0.0 0.0.0.0 192.168.16.1
```

Step 5: Define the application servers that require load balancing.

```
rserver host webserver1
 ip address 192.168.16.110
 inservice
rserver host webserver2
 ip address 192.168.16.111
 inservice
```

Step 6: Set up 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 7: 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 8: Configure the load-balancing policy and assign it to the VLAN interface.

```
class-map match-all http-vip
 2 match virtual-address 192.168.16.100 tcp eq www
policy-map type loadbalance first-match http-vip-lb
 class class-default
  serverfarm webfarm
policy-map multi-match int1116
 class http-vip
  loadbalance vip inservice
  loadbalance policy http-vip-lb
  loadbalance vip icmp-reply active
  nat dynamic 1 vlan 1116
interface vlan 1116
 service-policy input int1116
```

At this point, the application should be accessible via the VIP (192.168.16.100), 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 organizations improve availability, performance, and security of all applications. The Cisco ACE Application Control Engine provides core-server load-balancing services, advanced application acceleration, and security services in order to maximize application availability, performance, and security. It is coupled with unique virtualization capabilities, application-specific intelligence, and granular role-based administration in order to consolidate application infrastructure, reduce deployment costs, and minimize operational burdens.

Summary

This deployment guide is a reference design for Cisco customers and partners. It covers the Internet Edge component of Borderless Networks for Enterprise Organizations and is meant to be used in conjunction with the *Smart Business Architecture Borderless Networks for Enterprise Organizations LAN Deployment Guide* and *WAN Deployment Guide*, which can be found at 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, *SBA Borderless Networks for Enterprise Organizations Configuration Guide*, contains the specific configuration files from the products used in the Cisco lab testing and can be found on Cisco.com.

Notes

Appendix A: Enterprise Organizations Deployment Product List

Functional Area	Product	Part Numbers	Software Version
Internet Edge 5K			
Firewall	ASA 5510 or ASA 5520 or ASA 5540	ASA5510-AIP10-SP-K9 ASA5520-AIP20-K9 ASA5540-AIP40-K9	8.4.2
IPS	SSM-AIP-10 or SSM-AIP-20 or SSM-AIP-40	*part of the firewall bundle	7.0.5aE4
Software license for main ASA FW	250 or 500 SSL Session Software license	ASA5500-SSL-250 ASA5500-SSL-500	*as Firewall
Email Security	C370	C370-BUN-R-NA *Please consult Trusted Partner or IronPort Sales Team for pricing and licensing	Async OS 7.1.5-017
Web Security	S370	S370-BUN-R-NA *Please consult Trusted Partner or IronPort Sales Team for pricing and licensing	Async OS 7.1.2-080
Server Load Balancing	ACE 4710	ACE-4710-0.5F-K9	A5.1
Outside Switch	Catalyst 2960S	WS-C2960S-24TS-L	15.0(1)SE1
DMZ Switch	Catalyst 3750X	WS-C3750X-24T-S	15.0(1)SE1
Internet Edge 10K			
Firewall	ASA 5520 or ASA 5540	ASA5520-AIP20-K9 ASA5540-AIP40-K9	8.4.2
IPS	SSM-AIP-20 or SSM-AIP-40	*part of bundle above	7.0.5aE4

Functional Area	Product	Part Numbers	Software Version
VPN	ASA 5520 and 500 SSL seats or ASA 5540 and 1000 SSL seats	ASA5520-SSL500-K9 ASA5540-SSL1000-K9	8.4.2
Email Security	C370	C370-BUN-R-NA *Please consult Trusted Partner or IronPort Sales Team for pricing and licensing	Async OS 7.1.5-017
Web Security	S370	S370-BUN-R-NA *Please consult Trusted Partner or IronPort Sales Team for pricing and licensing	Async OS 7.1.2-080
Server Load Balancing	ACE 4710	ACE-4710-1F-K9	A5.1
Outside Switch	Catalyst 2960S	WS-C2960S-24TS-L	15.0(1)SE1
DMZ Switch	Catalyst 3750X	WS-C3750X-24T-S	15.0(1)SE1

Appendix B: Changes

This appendix summarizes the changes to this guide since the previous Cisco SBA series.

- In the Architecture Overview section, we integrated the Internet Edge Connectivity section, to simplify and clarify the structure of this guide.
- In The Firewall section, we added information about how to deploy the outside and DMZ switches. In the previous series, this information was not present.
- In the Remote Access VPN section, we rewrote the process to use a wizard-based deployment process for baseline deployment.
- In Internet Edge Server Load Balancing section, we added a management context on the Cisco ACE 4710 appliance.

Notes

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.**

B-0000124-1 12/11