



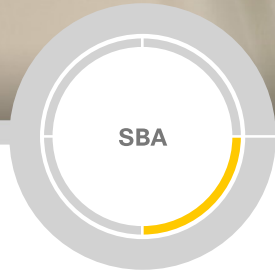
Newer Design Guide Available

Cisco Smart Business Architecture has become part of the Cisco Validated Designs program.

For up-to-date guidance on the designs described in this guide, see <http://cvddocs.com/fw/Aug13-180>

For information about the Cisco Validated Design program, go to <http://www.cisco.com/go/cvd>





Firewall and IPS Deployment Guide

● ● ● SMART BUSINESS ARCHITECTURE

February 2013 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 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.

The Release Notes for a series provides a summary of additions and changes made in the 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 February 2013 is the “February 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 [SBA feedback form](#).

If you would like to be notified when new comments are posted, an RSS feed is available from the SBA customer and partner pages.

Table of Contents

What's In This SBA Guide	1	Intrusion Prevention	41
Cisco SBA Borderless Networks.....	1	Business Overview.....	41
Route to Success.....	1	Technology Overview.....	41
About This Guide.....	1	Deployment Details.....	43
		Deploying IPS.....	44
Introduction	2	Intrusion Prevention Summary.....	56
Related Reading.....	2	Appendix A: Product List	57
Design Goals.....	2	Appendix B: Configuration Example	59
Architecture Overview	5	ASA Firewall 5545X.....	59
Internet Edge Connectivity.....	6	DMZ Switch 3750X.....	67
		Outside Switch 2960S.....	70
Firewall	9	Appendix C: Changes	72
Business Overview.....	9		
Technology Overview.....	9		
Deployment Details.....	10		
Configuring the Firewall.....	10		
Configuring Firewall High Availability.....	14		
Configuring Management DMZ.....	16		
Configuring the Firewall Internet Edge.....	23		
Configuring the Web DMZ.....	36		
Firewall Summary.....	40		

What's In This SBA Guide

Cisco SBA Borderless Networks

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.

Cisco SBA Borderless Networks is a comprehensive network design targeted at organizations with up to 10,000 connected users. The SBA Borderless Network architecture incorporates wired and wireless local area network (LAN) access, wide-area network (WAN) connectivity, WAN application optimization, and Internet edge security infrastructure.

Route to Success

To ensure your success when implementing the designs in this guide, you should first read any guides that this guide depends upon—shown to the left of this guide on the route below. As you read this guide, specific prerequisites are cited where they are applicable.

About This Guide

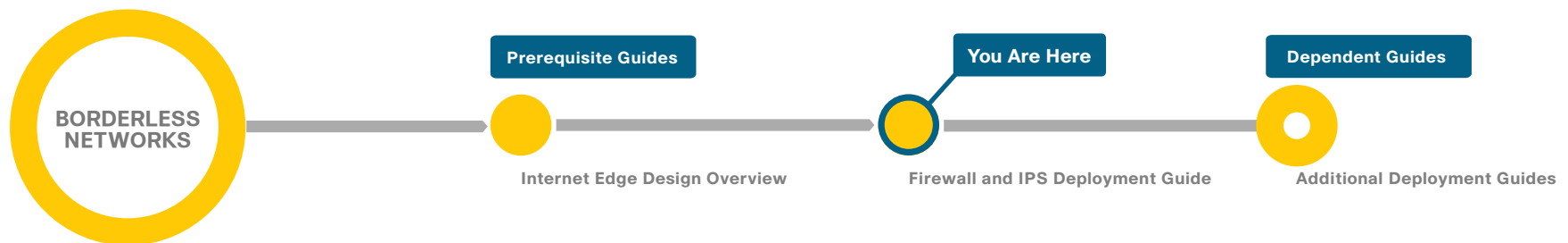
This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- **Business Overview**—Describes the business use case for the design. Business decision makers may find this section especially useful.
- **Technology Overview**—Describes the technical design for the business use case, including an introduction to the Cisco products that make up the design. Technical decision makers can use this section to understand how the design works.
- **Deployment Details**—Provides step-by-step instructions for deploying and configuring the design. Systems engineers can use this section to get the design up and running quickly and reliably.

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

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

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



Introduction

Cisco SBA Borderless Networks is a solid network foundation designed to provide networks with up to 10,000 connected users the flexibility to support new users and 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 *Firewall and IPS Deployment Guide* focuses on the Internet edge firewall and intrusion prevention system (IPS) security services that protect your organization's gateway to the Internet. Internet service-provider connectivity and routing options provide resiliency to the design. This guide covers the creation and use of DMZ segments for use with Internet-facing services such as a web presence. The IPS guidance covers Internet edge inline deployments as well as deployments of an intrusion detection system (IDS) on an internal distribution layer, also called *promiscuous* deployments.

Related Reading

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

The *Remote Access VPN Deployment Guide* and Remote Mobile Access Deployment Guide focus on provisioning the network to provide remote-access (RA) services. The deployments include VPN access as part of the Internet edge firewalls as well as the ability to deploy RA VPN services on separate dedicated devices.

The *Web Security Using Cisco WSA Deployment Guide* covers deploying the Cisco Web Security Appliance for clients accessing the Internet. This covers protection from malware and viruses as well as acceptable use controls for what sites are appropriate to be visited.

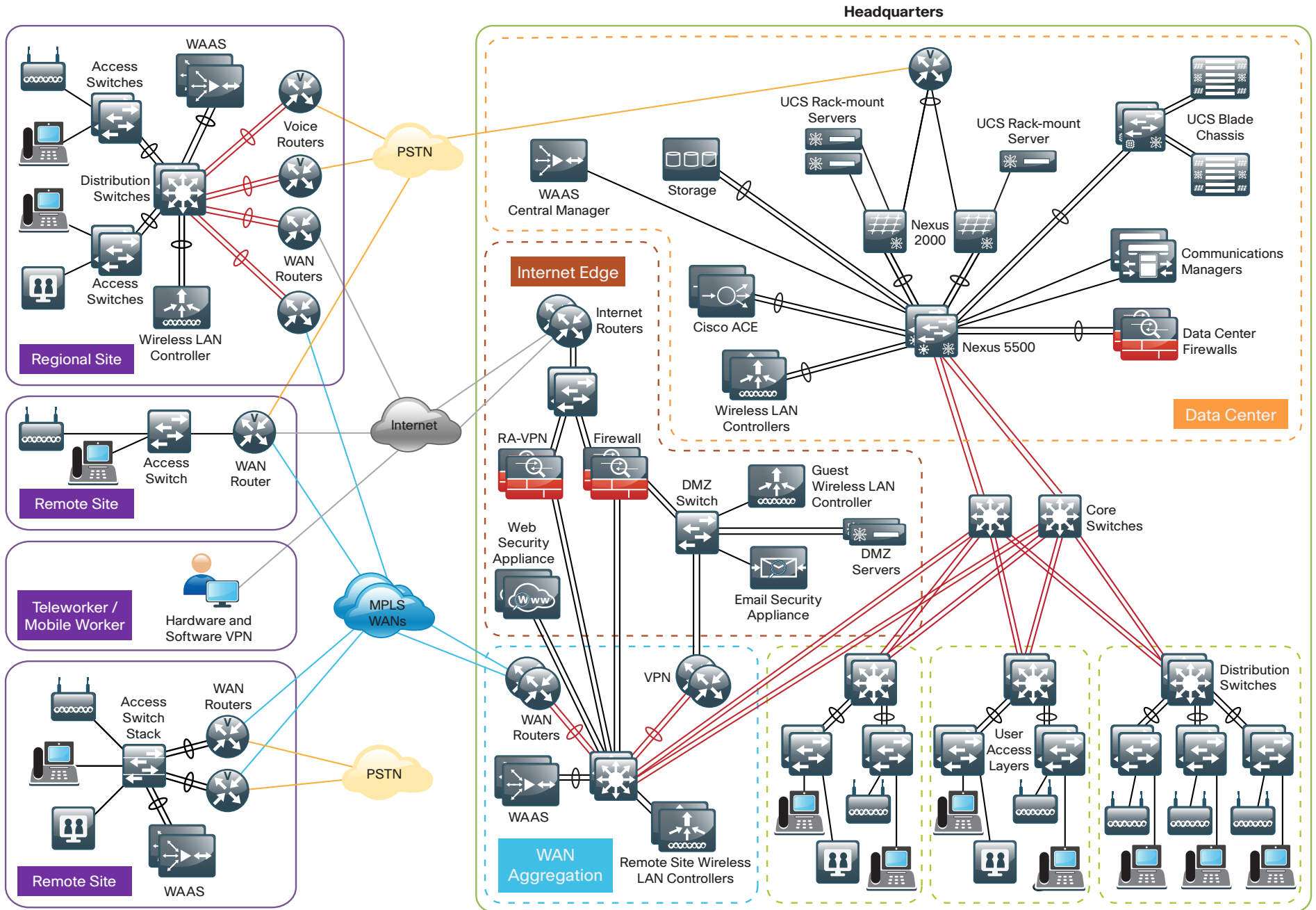
The *Cloud Web Security Using Cisco ASA Deployment Guide* covers deploying Cisco Cloud Web Security for clients accessing the Internet. This covers protection from malware and viruses as well as acceptable use controls for what sites are appropriate to be visited.

The *Email Security Using Cisco ESA Deployment Guide* covers deployment of the Cisco Email Security Appliance in order to help provide protection for the organization's email system. Inspection of inbound emails for spam and malicious content is the focus of the deployment. It also covers adding an email demilitarized zone (DMZ) to the Internet firewall in order to increase the overall security.

Design Goals

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

Figure 1 - Borderless Networks overview



2189

Ease of Deployment, Flexibility, and Scalability

Organizations with up 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 in order to ensure that interfaces between the plug-ins are well defined.

Resiliency and Security

One of the keys to maintaining a highly available network is building the appropriate resilience into the network links and platforms in order to guard against single points of failure in the network. The resilience in the Cisco SBA Internet edge 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 link or 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 Secure Shell (SSH) Protocol and HTTPS, as well as via Network Management System (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 quality of service (QoS) in order to support high-quality voice.
- Multicast is configured in the network in order 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, as configured in a teleworker deployment.

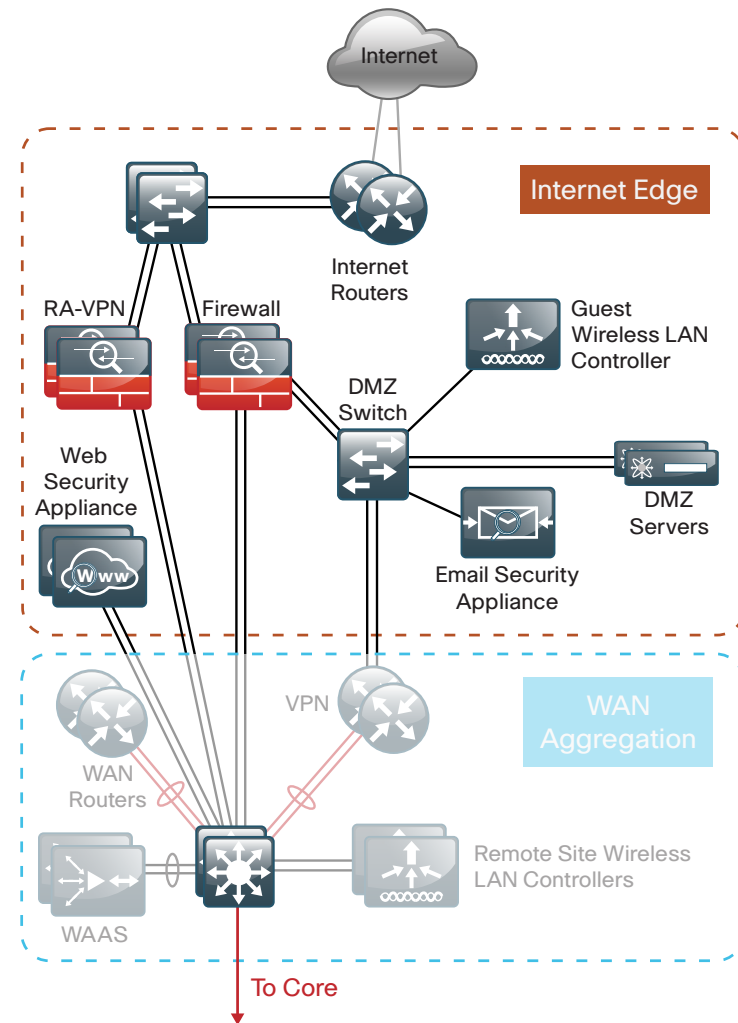
Architecture Overview

The *Firewall and IPS Deployment Guide* is a component of the larger Internet edge design, which uses a modular design model to break 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 functional blocks:

- **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) and DMZ creation.
- **Intrusion Prevention**—Inspects traffic traversing the Internet edge and looks 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 in order 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.

Figure 2 - Internet edge in the Borderless Networks design



3011

The primary differences in module design options are scale, performance, and resilience. To accommodate these requirements, each module of the Internet edge design is independent of the others, so you can mix and match the different design components to best meet your business requirements.

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.

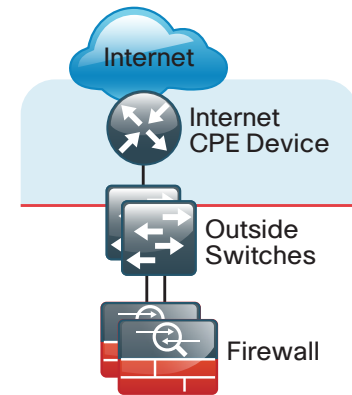
Internet connection speed, availability, and IP address space requirements are criteria that will shape an Internet connection design. The Internet connection must be able to accommodate an organization's requirements for data volume to the Internet, offer sufficient resiliency to meet service-level 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 address 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 3 - Internet connectivity demarcation for this design



Organizations deploying this design typically fall into the following Internet connection speed ranges.

Table 1 - Internet connection speed requirements

Number of connected users	Internet connection speed
Up 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 in order 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.

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 dual ISP 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 dual ISP design 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 up 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 dual ISP design 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 typically sufficient for organizations of up to 10,000 connected users that are not hosting critical content or eCommerce in their DMZ. In the dual ISP design, Cisco Adaptive Security Appliance (Cisco ASA) firewalls send Internet Control Message Protocol (ICMP) probes to an Internet IP address. 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 the users' Internet access and email (with an appropriately configured DNS). Further detail on configuration of this capability will be addressed in the 'Firewall' and 'Intrusion Prevention' sections of this document.



Reader Tip

The dual ISP design does not address multi-homed routing options, for example, 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

Notes

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 within 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 organization's 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 ensure 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

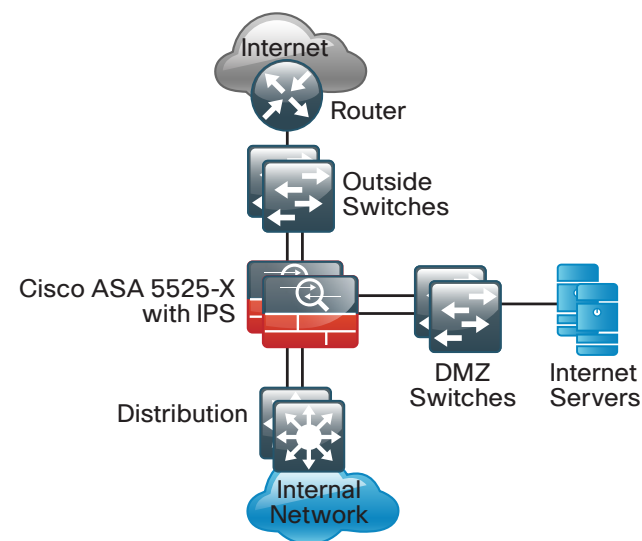
The Cisco ASA firewall family sits between the organization's internal network and the Internet and is a fundamental infrastructural component that minimizes the impact of network intrusions while maintaining worker productivity and data security.

This design uses Cisco ASA 5500-X Series Adaptive Security Appliances for Internet edge firewall security. They are configured in an active/standby pair for high availability in order to ensure that Internet access is only minimally impacted by firewall software maintenance or hardware failure. Cisco ASAs are configured in routing mode. They apply Network Address Translation (NAT) and firewall policy, and they host intrusion prevention system modules to detect and mitigate malicious or harmful traffic.

Two deployment options are discussed in order to address Internet access requirements for high availability. Each of these options also supports remote-access VPN with full deployment details, included in the *Cisco SBA—Borderless Networks Remote Access VPN Deployment Guide*.

One firewall design uses a single Internet connection with a Cisco ASA pair that provides the firewall functionality.

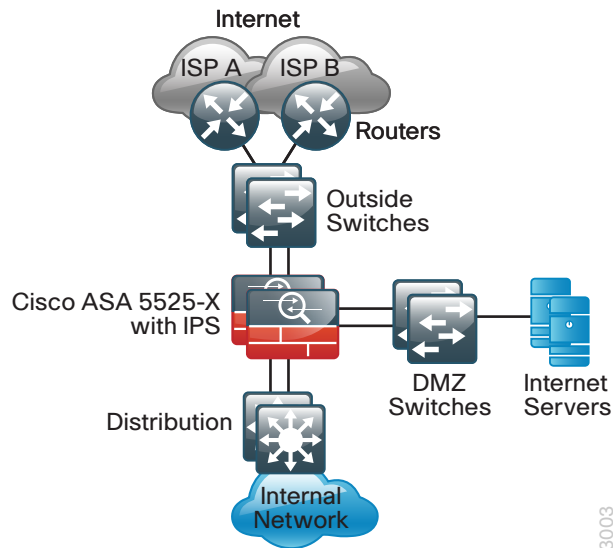
Figure 4 - Single ISP topology



3002

The larger firewall design uses dual Internet connections for resilient access to the Internet.

Figure 5 - Dual ISP topology



A good portion of the configuration described in this section is common to both the single and dual ISP designs. If a section describes configuration that is only used in one of the designs, this is mentioned in that section.

The configurations in this guide are for any of the one-rack-unit Cisco ASAs.

Hardware applied in these design is selected based on the following performance values. It is important to note that Internet connection speed is not the only data point when considering Cisco ASA device performance. To choose the correct platform, you must consider traffic that traverses the firewall from the internal network to the DMZ as well as inter-DMZ traffic.

Table 2 - Cisco ASA Family device performance

Cisco ASA Family product	Real-world firewall throughput (EMIX)
Cisco ASA 5512-X	500 Mbps
Cisco ASA 5515-X	600 Mbps
Cisco ASA 5525-X	1 Gbps
Cisco ASA 5545-X	1.5 Gbps

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 NTP and logging
6. Configure device-management protocols

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 pair needs to be configured. The “Configuring Firewall High Availability” process will set up high availability 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. To support future use, the connections from Cisco ASAs to the inside LAN distribution switches are configured as trunks.

An 802.1Q trunk is used for the connection to the Internet edge firewall, which allows the distribution switch to provide the Layer 3 services to all the VLANs defined on the firewall. The VLANs allowed on the trunk are pruned to only the VLANs that are active on the firewall.



Reader Tip

This procedure assumes that the distribution switch has already been configured following the guidance in the *Cisco SBA—Borderless Networks 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 on the LAN distribution switch.

```
vlan 300
  name InternetEdge
!
```

Step 2: Configure Layer 3 using a switched virtual interface (SVI). This allows devices in the VLAN to communicate with the rest of the network.

```
interface vlan 300
  description Internet Edge SVI
  ip address 10.4.24.1 255.255.255.224
  no shutdown
```

Step 3: Configure the interfaces that are connected to the Internet edge firewall.

```
interface GigabitEthernet1/0/24
  description IE-ASA5545Xa Gig0/0
!
interface GigabitEthernet2/0/24
  description IE-ASA5545Xb Gig0/0
!
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 300
  switchport mode trunk
  spanning-tree portfast trunk
  macro apply EgressQoS
  logging event link-status
  logging event trunk-status
  no shutdown
```

Cisco Catalyst 6500 uses the command **spanning-tree portfast edge trunk** to enable portfast on a trunk port. Catalyst 4500 does not require the **switchport trunk encapsulation dot1q** command.

Step 4: If your network has a collapsed core and distribution, proceed to the next step.

If your network uses separate distribution and core layers, 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 5: 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. The interface is configured as a VLAN trunk port in order to allow flexibility to add additional connectivity.

Step 1: Configure the appliance host name.

```
hostname IE-ASA5545X
```

Step 2: Configure the appliance interface that is connected to the internal LAN distribution switch as a subinterface on VLAN 300.

```
interface GigabitEthernet0/0
  no shutdown
!
interface GigabitEthernet0/0.300
  vlan 300
  nameif inside
  ip address 10.4.24.30 255.255.255.224
```

Step 3: Enable the dedicated management interface and remove any IP address that might be applied. This interface will only be used for IPS management.

```
interface Management0/0
  nameif IPS-mgmt
  no ip address
  no shutdown
```

Step 4: Configure an administrative username and password.

```
username admin password [password] privilege 15
```



Tech Tip

All passwords in this document are examples and should not be used in production configurations. Follow your organization's policy, or if no policy exists, create a password using a minimum of 8 characters with a combination of uppercase, lowercase, and numbers.

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

(Optional)

As networks scale in the number of devices to maintain, it poses an operational burden to maintain local user accounts on every device. A centralized authentication, authorization, and accounting (AAA) service reduces operational tasks per device and provides an audit log of user access, for security compliance and root-cause analysis. When 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 Server (ACS). Configuration of Cisco Secure ACS is discussed in the *Cisco SBA—Borderless Networks Device Management Using ACS Deployment Guide*.

TACACS+ is the primary protocol used to authenticate management logins on the infrastructure devices to the AAA server. A local AAA user database was defined already to provide a fallback authentication source in case the centralized TACACS+ server is unavailable.

Step 1: Configure the TACACS+ server.

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

Step 2: 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 3: Configure the appliance to use AAA 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 NTP and logging

Logging and monitoring are critical aspects of network security devices in order 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 to the device through Cisco ASDM; the appliance can offer controlled Cisco ASDM access for a single address or management subnet (in this case, 10.4.48.0/24).

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 10.4.48.0 255.255.255.0 inside
ssh 10.4.48.0 255.255.255.0 inside
ssh version 2
```

Step 2: Specify the list of supported SSL encryption algorithms for ASDM.

```
ssl encryption aes256-sha1 aes128-sha1 3des-sha1
```

Step 3: 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 resilience on primary firewall
2. Configuring standby firewall for resilience

Cisco ASAs 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 appliances in active/active configuration). In the event that the active appliance fails or needs to be taken out of service for maintenance, the secondary appliance assumes all active firewall, IPS, and VPN functions. In an active/standby configuration, only one device is passing traffic at a time; thus, 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 IPS (if the software module is installed). For failover to be enabled, the secondary Cisco ASA unit needs to be powered up and cabled to the same networks as the primary unit.

One interface on each Cisco 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 through 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, 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 resilience on primary firewall

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, which enables 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 high availability 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: Tune the failover poll timers to minimize the downtime experienced during failover.

```
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 shutdown
```

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

```
interface GigabitEthernet0/0.300
ip address 10.4.24.30 255.255.255.224 standby 10.4.24.29
monitor-interface inside
```

Procedure 2 Configuring standby firewall for resilience

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

```
failover
```

Step 2: Configure the Cisco ASA as the secondary appliance of the high availability 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: Tune the failover poll timers to minimize the downtime experienced during failover.

```
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 shutdown
```

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

```
IE-ASA5545X# 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.

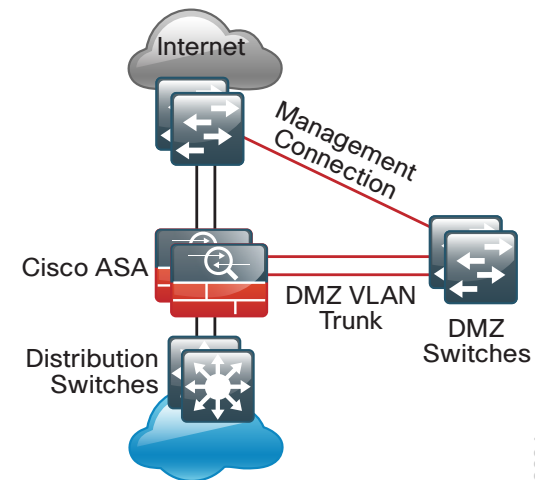
One of those special circumstances is for device management. However, the security policy on the firewall must still limit what traffic should be allowed inside from the DMZ because devices in the DMZ can be a security risk for the internal network.

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. In this architecture, the trunk connects the appliances to a Cisco Catalyst 3750-X Series switch stack that provides resiliency.

The DMZ interface on the Cisco ASA is assigned an IP address, which will be the default gateway for each 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 management of the switch.

Figure 6 - DMZ VLAN topology and services



3004

Procedure 1

Configure the DMZ switch

The DMZ switch in this deployment is a pair of Cisco Catalyst 3750-X Series switches in a stacked configuration. The configuration below is complete for the features required for the DMZ switch. This configuration is taken from the *Cisco SBA—Borderless Networks LAN Deployment Guide*.

To make consistent deployment of QoS easier, each platform defines a macro that you will use in later procedures in order to apply the platform-specific QoS configuration.

As networks scale in the number of devices to maintain, it poses an operational burden to maintain local user accounts on every device. A centralized authentication, authorization, and accounting (AAA) service reduces operational tasks per device and provides an audit log of user access, for security compliance and root cause analysis. When AAA is enabled for access control, AAA controls all management access to the network infrastructure devices (SSH and HTTPS). This procedure provides optional guidance for configuring the device to use AAA services in order to authenticate users.



Reader Tip

The AAA server used in this architecture is the Cisco Secure Authentication Control Server. For details about Cisco Secure ACS configuration, see the *Cisco SBA—Device Management Using ACS Deployment Guide*.

TACACS+ is the primary protocol used to authenticate management logins on the infrastructure devices to the AAA server. In Step 12, 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: Set the stack master switch.

```
switch [switch number] priority 15
```

Step 2: Ensure that the original master MAC address remains the stack MAC address after a failure.

```
stack-mac persistent timer 0
```

Step 3: Because AutoQoS might not be configured on this device, manually configure the global QoS settings:

```
mls qos map policed-dscp 0 10 18 to 8
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue input bandwidth 70 30
mls qos srr-queue input threshold 1 80 90
mls qos srr-queue input priority-queue 2 bandwidth 30
mls qos srr-queue input cos-map queue 1 threshold 2 3
mls qos srr-queue input cos-map queue 1 threshold 3 6 7
mls qos srr-queue input cos-map queue 2 threshold 1 4
mls qos srr-queue input dscp-map queue 1 threshold 2 24
mls qos srr-queue input dscp-map queue 1 threshold 3 48 49 50
51 52 53 54 55
mls qos srr-queue input dscp-map queue 1 threshold 3 56 57 58
59 60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 32 33 40
41 42 43 44 45
mls qos srr-queue input dscp-map queue 2 threshold 3 46 47
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
mls qos srr-queue output cos-map queue 2 threshold 1 2
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40
41 42 43 44 45
mls qos srr-queue output dscp-map queue 1 threshold 3 46 47
mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18
19 20 21 22 23
mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28
29 30 31 34 35
mls qos srr-queue output dscp-map queue 2 threshold 1 36 37 38
39
mls qos srr-queue output dscp-map queue 2 threshold 2 24
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50
51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58
```

```

59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3
4 5 6 7
mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11
13 15
mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
mls qos queue-set output 1 threshold 1 100 100 50 200
mls qos queue-set output 1 threshold 2 125 125 100 400
mls qos queue-set output 1 threshold 3 100 100 100 3200
mls qos queue-set output 1 threshold 4 60 150 50 200
mls qos queue-set output 1 buffers 15 25 40 20
mls qos
!
macro name EgressQoS
  mls qos trust dscp
  queue-set 1
  srr-queue bandwidth share 1 30 35 5
  priority-queue out
@
!

```

Step 4: Configure the device hostname.

```
hostname DMZ-3750X
```

Step 5: Configure VLAN Trunking Protocol (VTP) transparent mode.

```
vtp mode transparent
```

Step 6: Enable Rapid Per-VLAN Spanning-Tree (PVST+).

```
spanning-tree mode rapid-pvst
```

Step 7: Enable Unidirectional Link Detection (UDLD).

```
udld enable
```

Step 8: Set EtherChannels to use the traffic source and destination IP address.

```
port-channel load-balance src-dst-ip
```

Step 9: Configure device management protocols.

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

```

ip ssh version 2
no ip http server
ip http secure-server
line vty 0 15
  transport input ssh
  transport preferred none
snmp-server community cisco RO
snmp-server community cisco123 RW

```

Step 10: If your network operational support is centralized and you would like to increase network security, use an access list to limit the networks that can access the device. In this example, only devices on the 10.4.48.0/24 network will be able to access the device via SSH or SNMP.

```

access-list 55 permit 10.4.48.0 0.0.0.255
line vty 0 15
  access-class 55 in
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55

```

Step 11: Configure DNS for host lookup.

```
ip name-server 10.4.48.10
```

Step 12: Configure local login and password.

```

username admin password cisco123
enable secret cisco123
service password-encryption
aaa new-model

```

Step 13: If you are using AAA services, configure centralized user authentication.

```

tacacs server TACACS-SERVER-1
address ipv4 10.4.48.15
key SecretKey
!
aaa group server tacacs+ TACACS-SERVERS
  server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local

```

```
aaa authorization exec default group TACACS-SERVERS local
aaa authorization console
ip http authentication aaa
```

Step 14: Configure a synchronized clock.

```
ntp server 10.4.48.17
!
clock timezone PST -8
clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

Step 15: Configure the management VLAN and set the DMZ switch to be the spanning tree root for the management VLAN.

```
vlan 1123
name dmz-mgmt
spanning-tree vlan 1-4094 root primary
```

Step 16: Configure the interfaces that connect to the Cisco ASA firewalls.

```
interface GigabitEthernet1/0/24
description IE-ASA5545Xa Gig0/1
!
interface GigabitEthernet2/0/24
description IE-ASA5545Xb Gig0/1
!
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1123
switchport mode trunk
spanning-tree portfast trunk
macro apply EgressQoS
logging event link-status
logging event trunk-status
no shutdown
```

Step 17: 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 18: Configure the appliance as the DMZ switch's default route.

```
ip default-gateway 192.168.23.1
```

Step 19: Configure bridge protocol data unit (BPDU) Guard globally to protect portfast-enabled interfaces.

```
spanning-tree portfast bpduguard default
```

Procedure 2

Configure the demilitarized zone interface

Step 1: Connect to Cisco Adaptive Security Device Manager (ASDM) by navigating to <https://10.4.24.30>, and then logging in with your username and password.

Step 2: Navigate to **Configuration > Device Setup > Interfaces**.

Step 3: Select the interface that is connected to the DMZ switch, and then click **Edit** (Example: GigabitEthernet0/1). The Edit Interface dialog box appears.

Step 4: Select **Enable Interface**, and then click **OK**.

Step 5: In the Interface pane, click **Add**, and then choose **Interface**.

Step 6: On the Add Interface dialog box, in the **Hardware Port** list, select the interface configured in Step 3. (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)

The screenshot shows the 'Add Interface' dialog box with the following configuration:

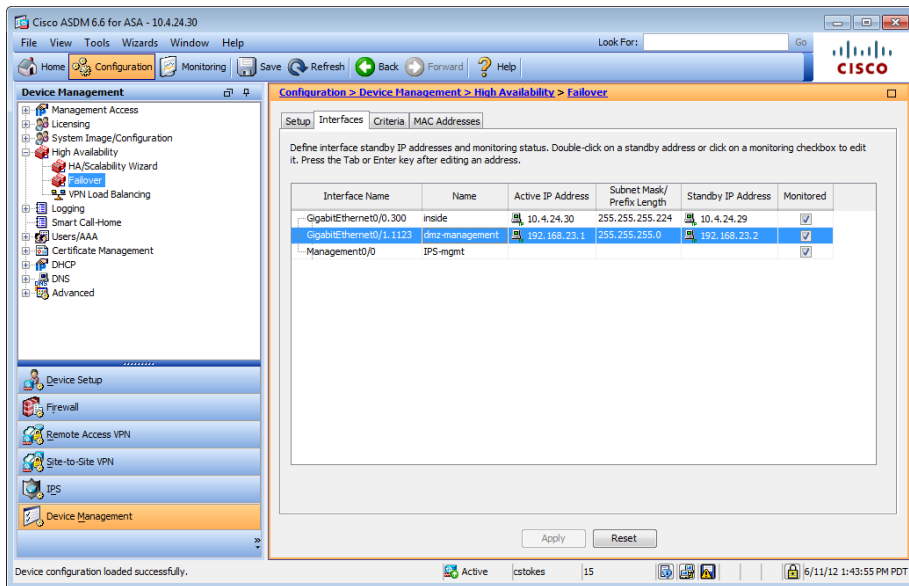
- Hardware Port: GigabitEthernet0/0
- VLAN ID: 1123
- Subinterface ID: 1123
- Interface Name: dmz-management
- Security Level: 50
- Dedicate this interface to management only
- Channel Group:
- Enable Interface
- IP Address: Use Static IP, Obtain Address via DHCP, Use PPPoE
- IP Address: 192.168.23.1
- Subnet Mask: 255.255.255.0
- Description: DMZ Management - For network device management

Step 13: Click **OK**.

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**.



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**, and then choose **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)

Procedure 3

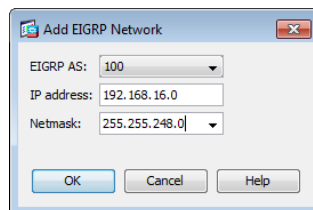
Configure the DMZ routing

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

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

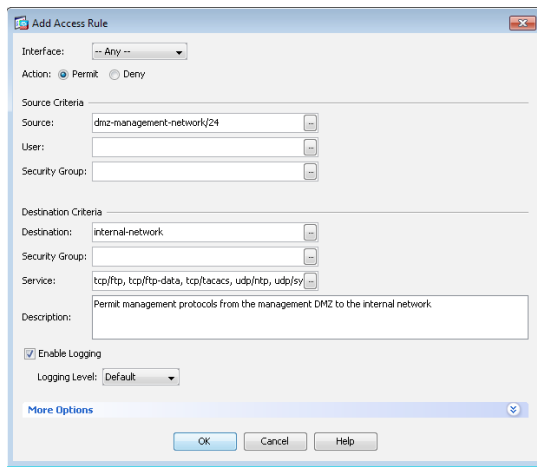
Step 3: In the Add EIGRP Network dialog box, in the **IP Address** box, enter the address that summarizes all DMZ networks. (Example: 192.168.16.0)

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



Step 5: In the Setup pane, click **Apply**. This saves the configuration.

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



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 this design can be summarized as 192.168.16.0/21.

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

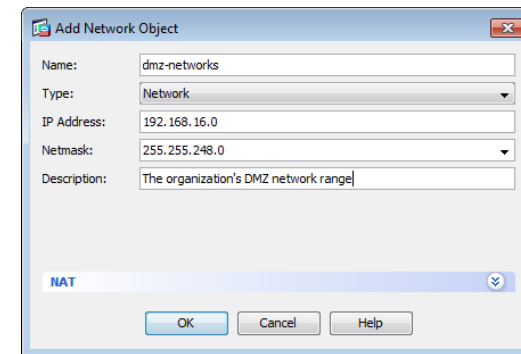
Step 9: Click **Add > Network Object**.

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). Click **Apply**.



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

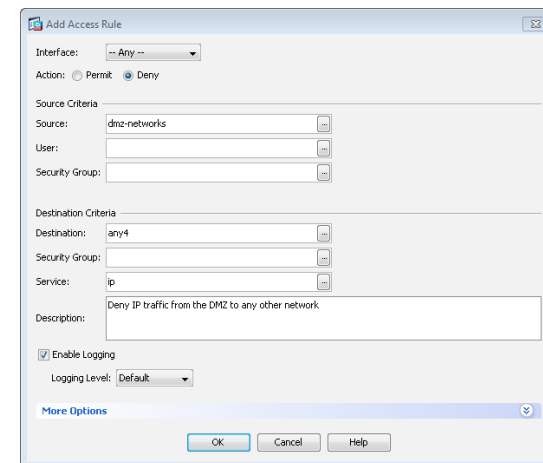
Step 14: Navigate to **Configuration > Firewall > Access Rules**.

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, for **Destination** select **any4**, and then click **OK**. (Example dmz-networks)



Step 19: In the Access Rules pane, click **Apply**. This saves the configuration.

Process

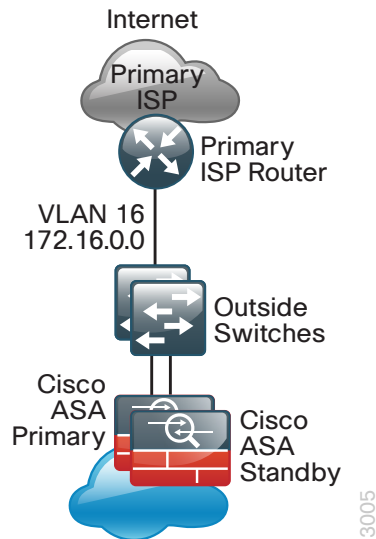
Configuring the Firewall Internet Edge

1. Configure the outside switch
2. Configure Cisco ASA outside connectivity
3. Configure address translation
4. Configure security policy

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

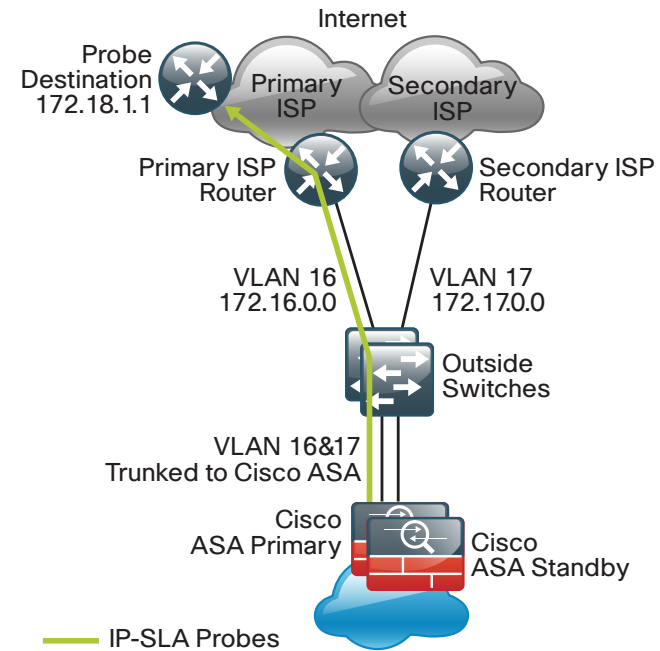
- Single ISP uses a single Internet connection via one router that carries the Internet traffic.

Figure 7 - Single ISP connectivity



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

Figure 8 - Dual 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* 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 (for example, **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 the application 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 it exposes 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 (for example, **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 Cisco ASA, the Cisco 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. Cisco IPS concepts and configuration are discussed in the Intrusion Prevention chapter in this document. Cisco WSA concepts and configuration are discussed in the *Cisco SBA—Borderless Networks Web Security Using Cisco WSA Deployment Guide*.

Procedure 1 Configure the outside switch

If you already have a switch on the outside into which you are allowed to plug both Cisco ASAs, then you can skip this procedure. This switch could be ISP-provided gear, such as a cable modem with a 4-port switch or similar. The only requirement in single ISP mode is that both Cisco ASAs' outside interfaces have to be plugged into the same Layer-2 domain in order to allow failover to function. In this deployment, a trunked outside interface is used, even in single ISP mode, to allow easier migration to dual ISP mode later. If you are using an outside switch that doesn't support trunking, you will need to assign the outside IP address directly to the interface of the appliance.

This procedure includes configuration steps for both single ISP and dual ISP designs.

The outside switch in this deployment is a pair of Cisco Catalyst 2960-S switches in a stacked configuration. The configuration below is complete for the features required for the outside switch. This configuration is taken from the *Cisco SBA—Borderless Networks LAN Deployment Guide*.

To make consistent deployment of QoS easier, we define a macro that you will use in later steps to apply the specific QoS configuration.

Step 1: Set the stack master switch.

```
switch [switch number] priority 15
```

Step 2: Ensure that the original master MAC address remains the stack MAC address after a failure.

```
stack-mac persistent timer 0
```

Step 3: Because AutoQoS might not be configured on this device, manually configure the global QoS settings:

```
mls qos map policed-dscp 0 10 18 to 8
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue input bandwidth 70 30
mls qos srr-queue input threshold 1 80 90
mls qos srr-queue input priority-queue 2 bandwidth 30
mls qos srr-queue input cos-map queue 1 threshold 2 3
mls qos srr-queue input cos-map queue 1 threshold 3 6 7
mls qos srr-queue input cos-map queue 2 threshold 1 4
mls qos srr-queue input dscp-map queue 1 threshold 2 24
mls qos srr-queue input dscp-map queue 1 threshold 3 48 49 50
mls qos srr-queue input dscp-map queue 1 threshold 3 51 52 53 54 55
mls qos srr-queue input dscp-map queue 1 threshold 3 56 57 58
mls qos srr-queue input dscp-map queue 2 threshold 3 32 33 40
mls qos srr-queue input dscp-map queue 2 threshold 3 41 42 43 44 45
mls qos srr-queue input dscp-map queue 2 threshold 3 46 47
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
mls qos srr-queue output cos-map queue 2 threshold 1 2
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
```

```

mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40
41 42 43 44 45
mls qos srr-queue output dscp-map queue 1 threshold 3 46 47
mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18
19 20 21 22 23
mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28
29 30 31 34 35
mls qos srr-queue output dscp-map queue 2 threshold 1 36 37 38
39
mls qos srr-queue output dscp-map queue 2 threshold 2 24
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50
51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58
59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3
4 5 6 7
mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11
13 15
mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
mls qos queue-set output 1 threshold 1 100 100 50 200
mls qos queue-set output 1 threshold 2 125 125 100 400
mls qos queue-set output 1 threshold 3 100 100 100 3200
mls qos queue-set output 1 threshold 4 60 150 50 200
mls qos queue-set output 1 buffers 15 25 40 20
mls qos
!
macro name EgressQoS
  mls qos trust dscp
  queue-set 1
  srr-queue bandwidth share 1 30 35 5
  priority-queue out
@
!
```

Step 4: Configure the device hostname to make it easy to identify the device.

```
hostname OUT-2960S
```

Step 5: Configure VTP transparent mode.

```
vtp mode transparent
```

Step 6: Configure Spanning-Tree (PVST+).

```
spanning-tree mode rapid-pvst
spanning-tree vlan 1-4094 root primary
```

Step 7: Enable Unidirectional Link Detection (UDLD).

```
udld enable
```

Step 8: Set EtherChannels to use the traffic source and destination IP address.

```
port-channel load-balance src-dst-ip
```

Step 9: Configure device management protocols.

```
ip domain-name cisco.local
ip ssh version 2
no ip http server
ip http secure-server
line vty 0 15
  transport input ssh
  transport preferred none
```

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 both for a read-only and a read-write community string.

```
snmp-server community cisco RO
snmp-server community cisco123 RW
```

Step 10: If your network operational support is centralized and you would like to increase network security, use an access list to limit the networks that can access the device. In this example, only devices on the 10.4.48.0/24 network will be able to access the device via SSH or SNMP.

```
access-list 55 permit 10.4.48.0 0.0.0.255
line vty 0 15
  access-class 55 in
!
snmp-server community cisco R0 55
snmp-server community cisco123 RW 55
```

Step 11: Configure DNS for host lookup.

```
ip name-server 10.4.48.10
```

Step 12: Configure local login and password.

```
username admin password c1sco123
enable secret c1sco123
service password-encryption
aaa new-model
```

Step 13: If you are using AAA services, configure centralized user authentication.

```
tacacs server TACACS-SERVER-1
address ipv4 10.4.48.15
key SecretKey
!
aaa group server tacacs+ TACACS-SERVERS
  server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization exec default group TACACS-SERVERS local
aaa authorization console
ip http authentication aaa
```

Step 14: Configure a synchronized clock.

```
ntp server 10.4.48.17
!
clock timezone PST -8
clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

Step 15: On the outside switch, configure the VLAN for the single or primary ISP.

```
vlan 16
name ISP-A
```

Step 16: Configure the interface that is connected to the single or primary ISP router.

```
interface GigabitEthernet1/0/23
description ISP-A
switchport access vlan 16
switchport host
no cdp enable
```

Step 17: Configure the interfaces that connect to the appliances.

```
interface GigabitEthernet1/0/24
description IE-ASA5545Xa Gig0/3
!
interface GigabitEthernet2/0/24
description IE-ASA5545Xb Gig0/3
!
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
switchport trunk allowed vlan 16
switchport mode trunk
spanning-tree portfast trunk
macro apply EgressQoS
logging event link-status
logging event trunk-status
no shutdown
```

Step 18: Configure the switch with an IP address. This enables the IP address to be managed via out-of-band connectivity.

```
interface FastEthernet0
  description to DMZ-3750X Gig1/0/17
  ip address 192.168.23.6 255.255.255.0
  no shutdown
```

Step 19: Configure the appliance as the DMZ switch's default route.

```
ip default-gateway 192.168.23.1
```

Step 20: 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-2960Sb Fas0
  !
interface range GigabitEthernet1/0/17, GigabitEthernet2/0/17
  switchport access vlan 1123
  switchport host
  no shutdown
```

Step 21: On the outside switch, configure BPDU Guard globally to protect portfast-enabled interfaces.

```
spanning-tree portfast bpduguard default
```

Step 22: If you are using a single ISP design, skip to the next procedure.

If you are using a dual ISP design, continue with this procedure.

Step 23: On the outside switch, add the VLAN for the backup ISP.

```
vlan 17
  name ISP-B
```

Step 24: Configure the interface that connects to the ISP router.

```
interface GigabitEthernet2/0/23
  description ISP-B
  switchport access vlan 17
  switchport host
  no cdp enable
```

Step 25: Configure the interfaces that connect to the appliances.

```
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
  switchport trunk allowed vlan add 17
  no shutdown
```

Procedure 2

Configure Cisco ASA outside connectivity

If you are using a non-trunked single ISP design, complete Option 1. If you are using a trunked design using either single or dual ISPs, complete Option 2.

Option 1. Using a non-trunked design

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://10.4.24.30>)

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**.

Step 5: Enter an **Interface Name**. (Example: outside)

Step 6: In the **Security Level** box, enter a value of **0**.

Step 7: Enter the interface **IP Address**. (Example: 172.16.130.124)

Step 8: Enter the interface **Subnet Mask**, and then click **OK**. (Example: 255.255.255.0)

The screenshot shows the 'Edit Interface' dialog box with the following details:

- Hardware Port: GigabitEthernet0/3
- Interface Name: outside
- 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

Step 9: On the Interface pane, click **Apply**.

Step 10: Navigate to **Configuration > Device Management > High Availability > Failover**.

Step 11: 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 12: Select **Monitored**, and then click **Apply**.

The screenshot shows the 'High Availability > Failover' configuration page with the following table:

Interface Name	Name	Active IP Address	Subnet Mask/Prefix Length	Standby IP Address	Monitored
GigabitEthernet0/0.300	inside	10.4.24.30	255.255.255.224	10.4.24.29	<input checked="" type="checkbox"/>
GigabitEthernet0/1.1123	dmz-management	192.168.23.1	255.255.255.0	192.168.23.2	<input checked="" type="checkbox"/>
GigabitEthernet0/3	outside	172.16.130.124	255.255.255.0	172.16.130.123	<input checked="" type="checkbox"/>
Management0/0	IPS-mgmt				<input type="checkbox"/>

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

Step 13: In **Configuration > Device Setup > Routing > Static Routes**, click **Add**.

Step 14: In the Add Static Route dialog box, in the **Interface** list, choose the interface edited in Step 2. (Example: outside)

Step 15: In the **Network** box, select **any4**.

Step 16: In the **Gateway IP** box, enter the primary Internet CPE's IP address, and then click **OK**. (Example: 172.16.130.126)

Add Static Route

IP Address Type: IPv4 IPv6

Interface:

Network: ...

Gateway IP: ... Metric:

Options

None

Tunneled (Default tunnel gateway for VPN traffic)

Tracked

Track ID: Track IP Address:

SLA ID: Target Interface:

Monitoring Options

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

Step 17: On the Static Routes pane, click **Apply**.

Option 2. Using a trunked design

When resilient Internet access (dual ISP) is required, the appliances' GigabitEthernet 0/3, which is configured as a VLAN trunk to the outside switch, is assigned an additional VLAN to use to connect to the secondary ISP. The VLAN trunk allows the appliance to use separate VLANs for the upstream Internet routers.

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: 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://10.4.24.30>)

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**.

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 enabled in Step 4. (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)

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

OK Cancel Help

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

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
GigabitEthernet0/0.300	inside	10.4.24.30	255.255.255.224	10.4.24.29	<input checked="" type="checkbox"/>
GigabitEthernet0/1.1123	dmz-management	192.168.23.1	255.255.255.0	192.168.23.2	<input checked="" type="checkbox"/>
GigabitEthernet0/3.16	outside-16	172.16.130.124	255.255.255.0	172.16.130.123	<input checked="" type="checkbox"/>
Management0/0	IPS-mgmt				<input type="checkbox"/>

Apply Reset

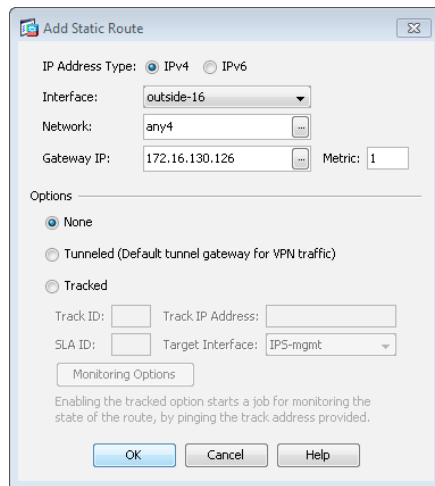
Next, you will create the default route to the primary Internet CPE's address.

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 9. (Example: outside-16)

Step 19: In the **Network** box, select **any4**.

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**.

Step 22: If you are using a single ISP design, skip to the next procedure. If you are using a dual ISP design, continue with this procedure.

Step 23: Navigate to **Configuration > Device Setup > Interfaces**.

Step 24: On the Interface pane, click **Add > Interface**.

Step 25: In the Add Interface dialog box, in the **Hardware Port** list, choose the interface configured in Step 4. (Example: GigabitEthernet0/3)

Step 26: In the **VLAN ID** box, enter the VLAN number for the resilient Internet VLAN. (Example: 17)

Step 27: In the **Subinterface ID** box, enter the VLAN number for the resilient Internet VLAN. (Example: 17)

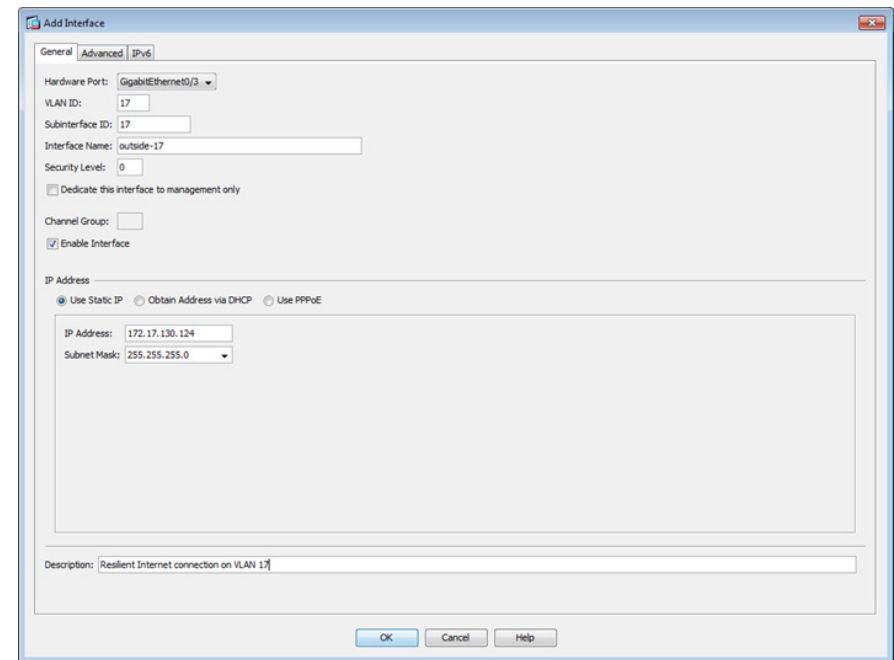
Step 28: Enter an **Interface Name**. (Example: outside-17)

Step 29: In the **Security Level** box, enter a value of **0**.

Step 30: Enter the interface **IP Address**. (Example: 172.17.130.124)

Step 31: Enter the interface **Subnet Mask**, and then click **OK**. (Example: 255.255.255.0)

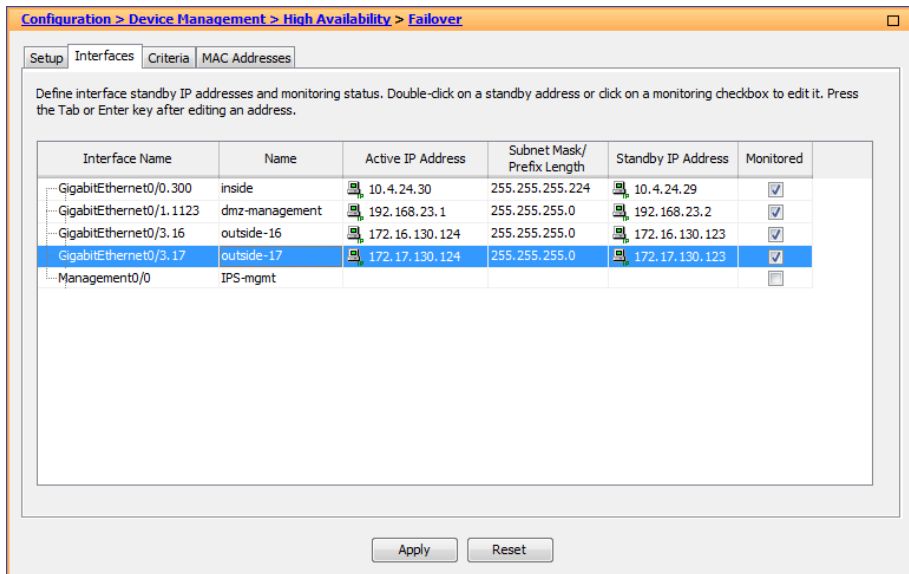
Step 32: On the Interface pane, click **Apply**.



Step 33: Navigate to **Configuration > Device Management > High Availability > Failover**.

Step 34: 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 35: Select **Monitored**, and then click **Apply**.



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

Step 36: Navigate to **Configuration > Device Setup > Routing > Static Routes**.

Step 37: Select the default route created in Step 20, and then click **Edit**.

Step 38: Verify that the Metric box remains set to 1.

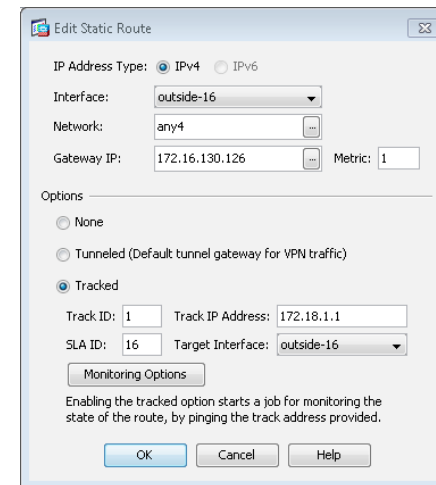
Step 39: In the Edit Static Route dialog box, in the **Options** pane, select **Tracked**.

Step 40: In the **Track ID** box, enter **1**.

Step 41: In the **Track IP Address** box, enter an IP address in the ISP's cloud. (Example: 172.18.1.1)

Step 42: In the **SLA ID** box, enter **16**.

Step 43: In the **Target Interface** list, select the primary Internet connection interface, and then click **OK**. (Example: outside-16)



Step 44: On the Information dialog box, click **OK**.

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

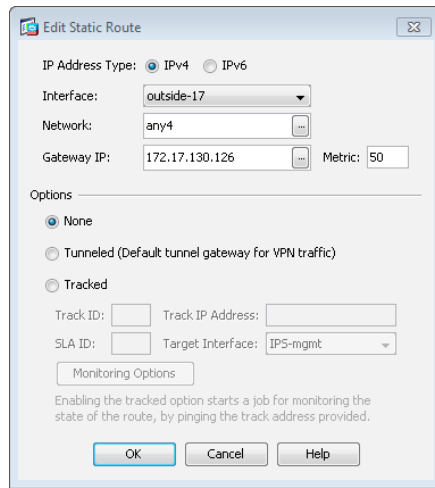
Step 45: In **Configuration > Device Setup > Routing > Static Routes**, click **Add**.

Step 46: In the Add Static Route dialog box, in the **Interface** list, select the resilient Internet connection interface created in Step 28. (Example: outside-17)

Step 47: In the **Network** box, select **any4**.

Step 48: In the **Gateway IP** box, enter the primary Internet CPE's IP address. (Example: 172.17.130.126)

Step 49: In the **Metric** box, enter **50**, and then click **OK**.



Step 50: On the Static Routes pane, click **Apply**.

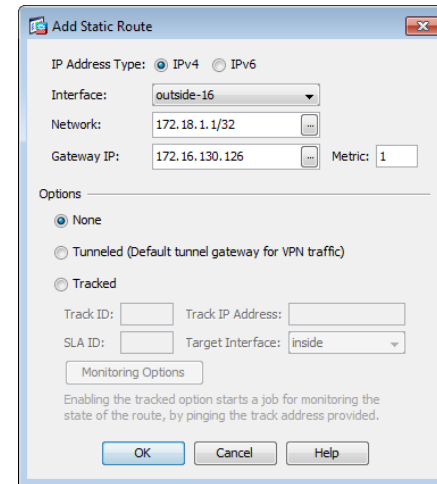
Next, you will add a host route for the tracked object via the Internet-CPE-1 address. This assures that probes to the tracked object will always use the primary ISP connection.

Step 51: In **Configuration > Device Setup > Routing > Static Routes**, click **Add**.

Step 52: In the Add Static Route dialog box, in the **Interface** list, select the primary Internet connection interface created in Step 9. (Example: outside-16)

Step 53: In the **Network** box, enter the IP address used for tracking in the primary default route. (Example: 172.18.1.1/32)

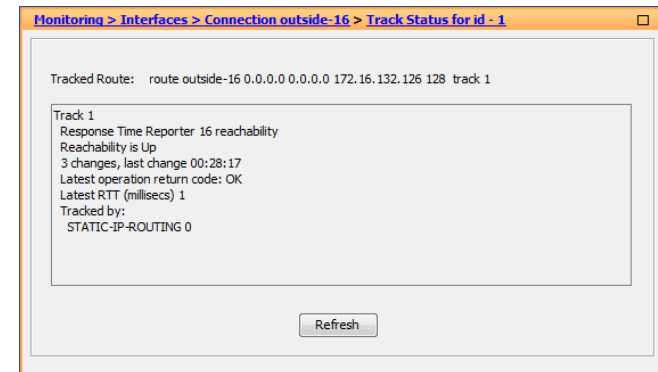
Step 54: In the **Gateway IP** box, enter the primary Internet CPE's IP address, and then click **OK**. (Example: 172.16.130.126)



Step 55: On the Static Routes pane, click **Apply**.

Step 56: In Cisco ASDM, refresh the configuration.

Step 57: If you want to monitor the reachability of the object, navigate to **Monitoring > Interfaces > Connection outside-16 > Track Status for id-1**.



Procedure 3 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 as if coming from 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 whether a single or dual ISP configuration is used. Most of the configuration is common to both designs, although there are some additional steps for configuring both outside interfaces in the dual ISP 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)

The screenshot shows the 'Add Network Object' dialog box. The 'Name' field contains 'internal-network-ISPa', 'Type' is 'Network', 'IP Version' is 'IPv4', 'IP Address' is '10.4.0.0', and 'Netmask' is '255.254.0.0'. The 'Description' field contains 'PAT traffic from inside out the primary Internet connection'. The 'NAT' pane is expanded, showing 'Add Automatic Address Translation Rules' checked, 'Type' set to 'Dynamic PAT (Hide)', and 'Translated Addr' set to 'outside-16'. Other options like 'Use one-to-one address translation', 'PAT Pool Translated Address', 'Round Robin', 'Extend PAT uniqueness to per destination instead of per interface', 'Translate TCP and UDP ports into flat range 1024-65535', 'Include range 1-1023', 'Fall through to interface PAT(dest intf): IPS-mgmt', and 'Use IPv6 for interface PAT' are unchecked. An 'Advanced...' button is visible at the bottom of the NAT pane. At the bottom of the dialog box are 'OK', 'Cancel', and 'Help' buttons.

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

Step 12: If you are using a single ISP design, continue to Procedure 4.

If you are using the dual ISP design, repeat Step 1 - Step 11 for the resilient Internet connection, using the correct input for the alternate Internet connection. (Example: internal-network-ISPb, outside-17)

Procedure 4 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**.

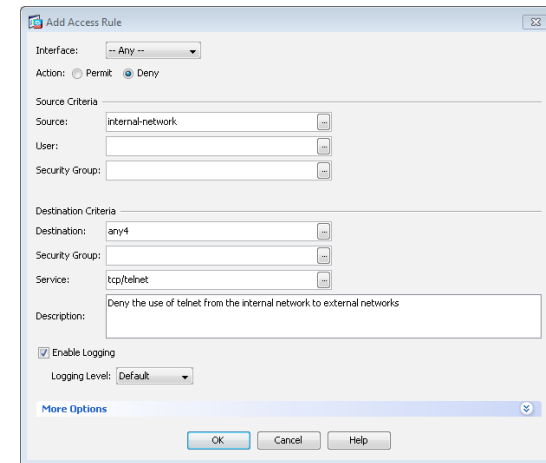
Step 3: In the Add Access Rule dialog box, in the **Interface** list, select **—Any—**.

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 Destination list, select **any4**.

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



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

Step 8: Click **Add > Add Access Rule**.

Step 9: In the Add Access Rule dialog box, in the **Interface** list, select **—Any—**.

Step 10: For **Action**, select **Permit**.

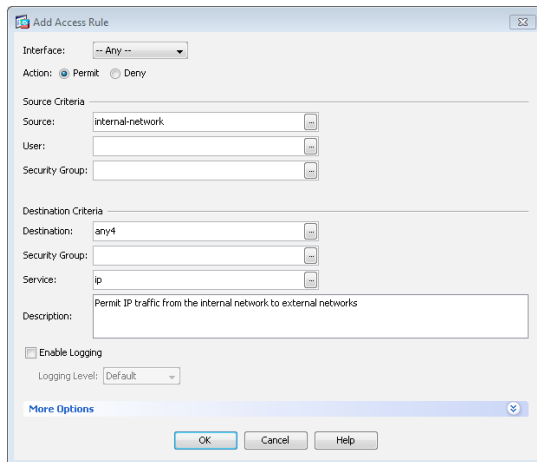
Step 11: In the **Source** list, select the network object that summarizes the internal networks. (Example: internal-network)

Step 12: Clear **Enable Logging**, and then click **OK**.



Tech Tip

Firewalls generate large amounts of log data. This access rule likely includes the majority of user Internet traffic, so by disabling logging, you significantly reduce the total amount of log data generated by the firewall. However, this also reduces visibility into user traffic, which may be used for analysis or troubleshooting.



Step 13: On the Access Rules pane, click **Apply**.

Process

Configuring the Web DMZ

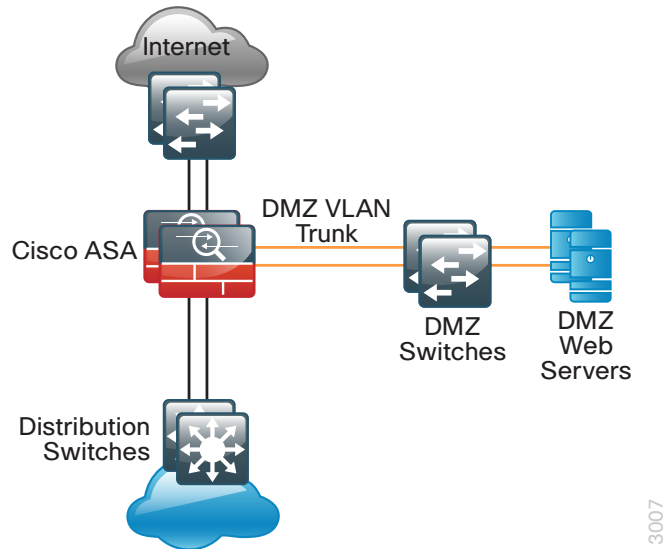
1. Configure the DMZ switch
2. Configure DMZ interface
3. Configure Network Address Translation
4. Configure security policy

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' 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 Cisco Catalyst 3750-X Series access-switch stack in order to provide resiliency. The DMZ VLAN interfaces on the appliance 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 9 - Web DMZ VLAN topology



The number of secure VLANs is arbitrary. The following deployment 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

This procedure assumes that the DMZ switch has already been configured following the guidance in the previous process Configuring Management DMZ.

Step 1: On the DMZ switch, configure the DMZ web VLAN.

```
vlan 1116
name dmz-web
```

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

```
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
switchport trunk allowed vlan add 1116
```

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

```
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: Connect to Cisco Adaptive Security Device Manager (ASDM) by navigating to <https://10.4.24.30>, and then logging in with your username and password.

Step 2: Navigate to **Configuration > Device Setup > Interfaces**.

Step 3: On the Interface pane, click **Add > Interface**.

Step 4: In the Add Interface dialog box, in the **Hardware Port** list, choose the interface connected to the DMZ switch. (Example: GigabitEthernet0/1)

Step 5: In the **VLAN ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1116)

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

Step 7: Enter an **Interface Name**. (Example: dmz-web)

Step 8: In the **Security Level** box, enter a value of 50.

Step 9: Enter the interface **IP Address**. (Example: 192.168.16.1)

Step 10: Enter the interface **Subnet Mask**, and then click **OK**. (Example: 255.255.255.0)

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

OK Cancel Help

Step 11: On the Interface pane, click **Apply**.

Step 12: Navigate to **Configuration > Device Management > High Availability > Failover**.

Step 13: 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 14: 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
GigabitEthernet0/0.300	inside	10.4.24.30	255.255.255.224	10.4.24.29	<input checked="" type="checkbox"/>
GigabitEthernet0/1.1116	dmz-web	192.168.16.1	255.255.255.0	192.168.16.2	<input checked="" type="checkbox"/>
GigabitEthernet0/1.1123	dmz-management	192.168.23.1	255.255.255.0	192.168.23.2	<input checked="" type="checkbox"/>
GigabitEthernet0/3.16	outside-16	172.16.130.124	255.255.255.0	172.16.130.123	<input checked="" type="checkbox"/>
GigabitEthernet0/3.17	outside-17	172.17.130.124	255.255.255.0	172.17.130.123	<input checked="" type="checkbox"/>
Management0/0	IPS-mgmt				<input type="checkbox"/>

Apply Reset

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 3 - DMZ address mapping

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

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

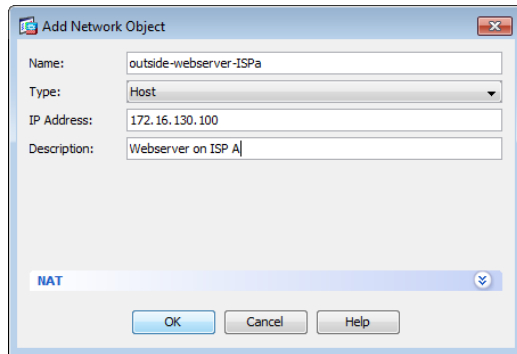
First, you will add a network object for the web server's IP address on the primary Internet connection.

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**.

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)

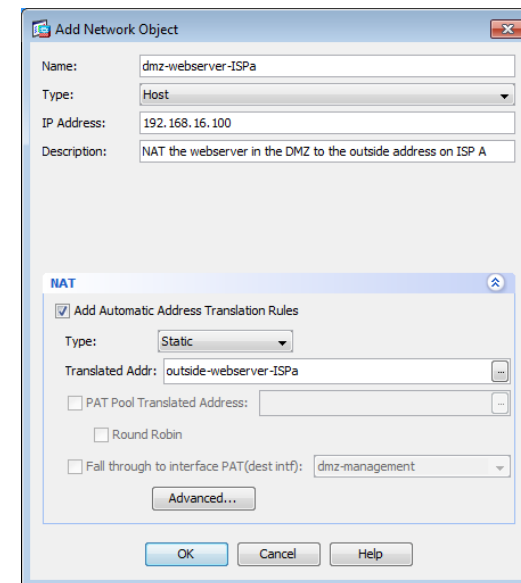
Step 9: In the **Type** list, select **Host**.

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.

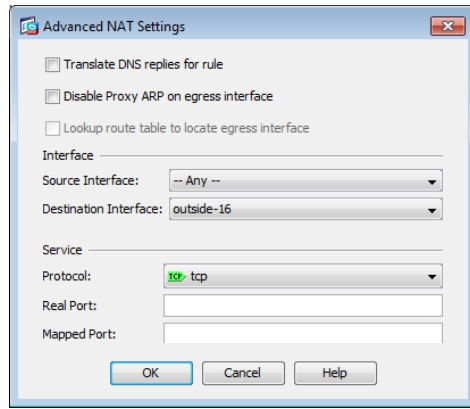
Step 12: Select **Add Automatic Address Translation Rules**.

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



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)



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 dual ISP design with a resilient Internet connection, repeat this procedure for the secondary Internet connection.

If you are using the single ISP design, proceed to Procedure 4.

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.



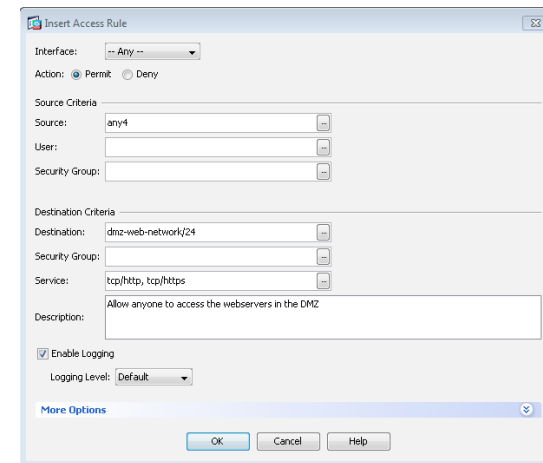
Step 3: Click **Add > Insert**.

Step 4: In the Insert 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**.

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.

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) in order to provide additional protection for the organization from the traffic that is permitted through the Internet edge firewall. Cisco IPS technology complements the firewall and inspects traffic permitted by the firewall policy, for attacks.

Cisco IPS devices come in two formats: standalone appliances and hardware or software modules inside a Cisco ASA firewall. The differences between the devices generally revolve around how the devices get the traffic they inspect. An appliance uses physical interfaces that exist as part of the network. A module receives traffic from the Cisco ASA firewall in which it resides, according to the policy defined on the firewall.

With either type of device, there are two deployment modes available: promiscuous (IDS) or inline (IPS). There are specific reasons for each deployment mode, based on risk tolerance and fault tolerance. *Inline* or *IPS mode* means that the IPS device sits inline on the traffic flow in order to inspect the actual packets, and if an alert is triggered that includes a drop action, the IPS device can drop the actual malicious packet. *Promiscuous* or *IDS mode* (note that an IPS device can operate in IDS mode) means that an external device is copying the packets to the IPS device. For an appliance, the way packets are copied is generally a network tap or a switch running a SPAN session. For a module, the copying happens at the Cisco ASA

firewall and is controlled by the Cisco ASA configuration. Because inline and promiscuous are operating modes, an IPS device can inspect traffic at multiple places, and each inspection point could be set up independently as inline or promiscuous.

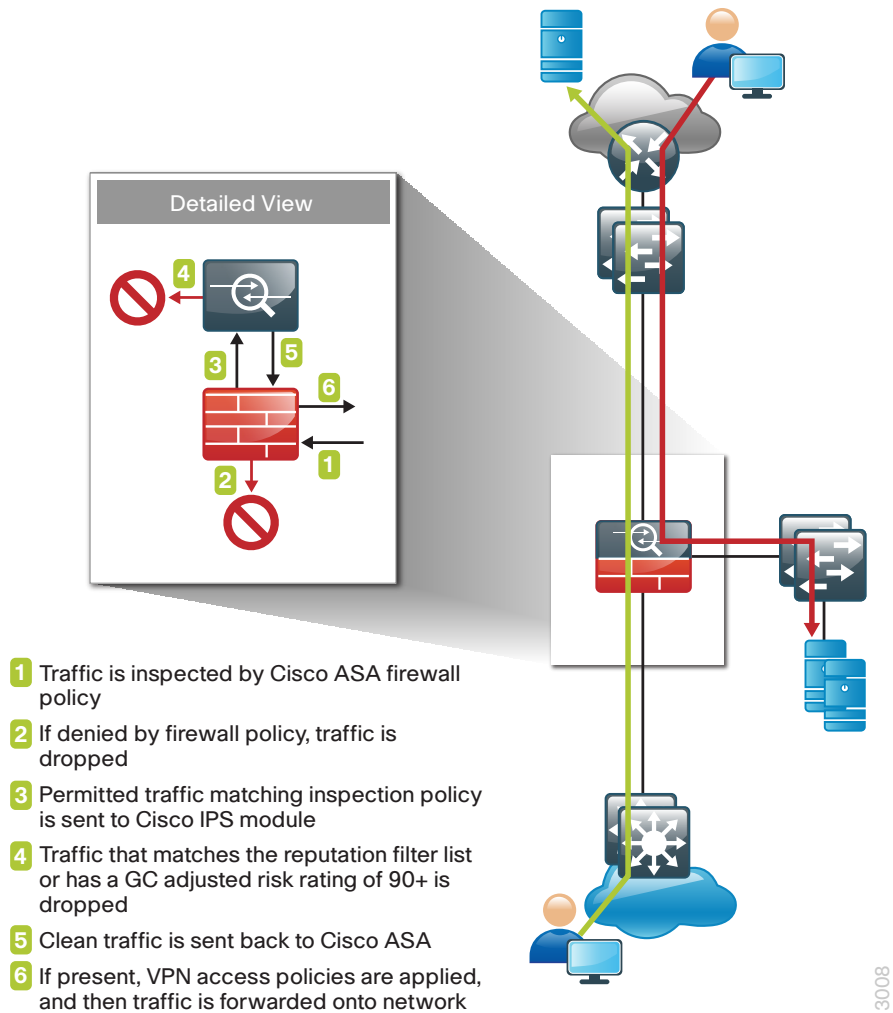
Using inline mode means that network traffic flows through an IPS device, and if the device fails or misbehaves, it will impact production traffic. The advantage inline mode offers is that when the sensor detects malicious behavior, the sensor can simply drop it. This allows the IPS device a much greater capacity to actually prevent attacks.

Using promiscuous mode means that the IPS device must use another inline enforcement device in order to stop malicious traffic. This means that for activity such as single-packet attacks (slammer worm over User Datagram Protocol), an IDS sensor could not prevent the attack from occurring. However, an IDS sensor can offer great value when identifying and cleaning up infected hosts.

This design uses Cisco ASA 5500 Series IPS Solution (software module inside Cisco ASA) at the Internet edge. The design offers several options that are based on the performance requirements of the organization. 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.

You will also deploy standalone Cisco IPS 4300 Series Sensors in promiscuous mode. The ability to deploy a sensor internally on the network in order to watch traffic on any distribution switch can be very valuable. These sensors can be used to watch traffic going to and from the WAN network, traffic on the wireless network, or even traffic on a B2B network to a partner.

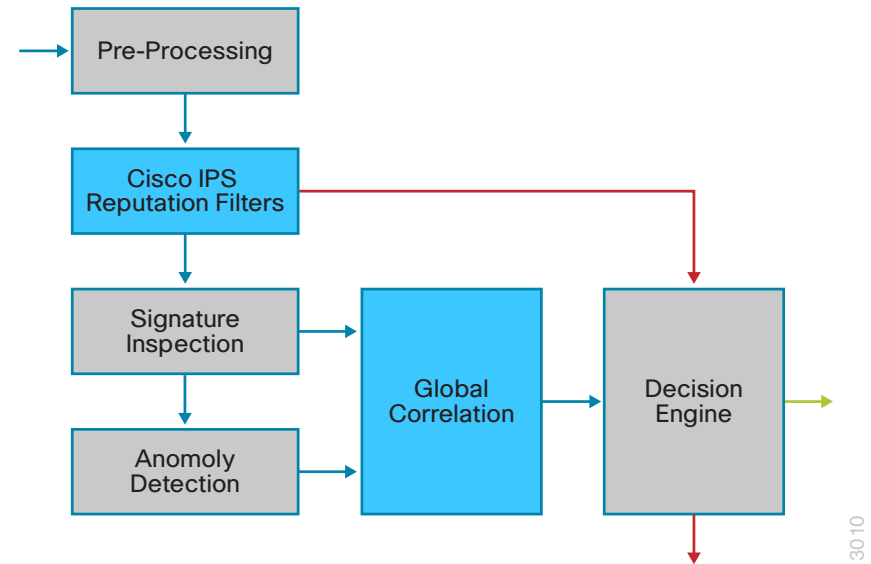
Figure 10 - Packet flow through a Cisco ASA firewall and Cisco IPS module



3008

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

Figure 11 - IPS processing flowchart



3010

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.

Because Global Correlation Inspection depends on actual public IP addresses to function, any sensor that is deployed internally and sees only private addresses should have Global Correlation Inspection disabled because it will not add any value.

The Cisco IPS module has the capability to send data to the Cisco SensorBase network. This data feeds into the Global Correlation database in order to increase reputation fidelity.


There are three modes for network participation:

- **Off**—The network participation server does not collect data, track statistics, or try to contact the Cisco SensorBase network.
- **Partial Participation**—The network participation server collects data, tracks statistics, and communicates with the Cisco SensorBase network. Data considered to be potentially sensitive is filtered out and never sent.
- **Full Participation**—The network participation server collects data, tracks statistics, and communicates with the Cisco SensorBase network. All data collected is sent.

Figure 12 - 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	96	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	97	99	100	100	100	100	100	100	100	100	100	100	100	100	100	100
	98	98	98	98	98	98	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	

3012



Reader Tip

For more information about how traffic moves through the Cisco ASA and IPS module combination, see the following: http://www.cisco.com/en/US/docs/security/asa/asa90/asdm70/configuration_guide/modules_ips.html#wp1087140

Deployment Details

In this deployment, you will deploy Cisco ASA IPS modules in inline mode in order to help block inbound attacks to the Internet services in the DMZ. You will also deploy a standalone IPS appliance in promiscuous mode on the inside of the network. This appliance will be attached to a distribution switch and will watch for possible malicious activity in the traffic traversing the switch. The appliance is deployed on the WAN aggregation switch so that it can inspect the traffic going between the campus and remote sites. This could just as easily be deployed to watch other LAN sites, the traffic from the DMVPN connection, wireless traffic (after it enters the wired LAN), or possibly partner connections. Because it is possible to send too much traffic to an IPS device (too much for either the port or the hardware to handle), it is important to size the device carefully. The following tables give estimated performance for different models.

Table 4 - Cisco IPS performance levels

Cisco IPS appliance model	Average inspection throughput
Cisco IPS 4345 Sensor	750 Mbps
Cisco IPS 4360 Sensor	1.25 Gbps
Cisco IPS 4510 Sensor	3 Gbps
Cisco IPS 4520 Sensor	5 Gbps

Table 5 - Cisco ASA 5500 Series IPS Solution performance levels

Cisco ASA 5500 Series IPS Solution module	Firewall + IPS throughput
Cisco ASA 5512-X	250 Mbps
Cisco ASA 5515-X	400 Mbps
Cisco ASA 5525-X	600 Mbps
Cisco ASA 5545-X	900 Gbps

For the Cisco IPS 4345 Sensor in this deployment, we use two 1-gigabit interfaces, where each is attached to one of the switches in the switch stack. If faster models are used, options include either using a ten-gigabit interface or using a port channel of 2 or more 1-gigabit interfaces (these options are switch-dependent, as some switches and code versions do not support using port channels as destinations for Switched Port Analyzer sessions).

The first step used to configure a Cisco ASA 5500 Series IPS Solution module is to session into the module from the firewall 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 completed through a GUI such as Cisco ASA Security Device Manager (ASDM) or the Cisco IPS Manager Express.

Configuring the Cisco IPS 4300 or 4500 Series appliance follows similar steps with the addition of one procedure in which you configure the switch to copy packets to the sensor's interface for inspection.

Use the following values when configuring IPS and IDS devices.

Table 6 - IPS device configuration

Device characteristics	IPS software module	IDS appliance
Location and mode	Internet edge IPS	Distribution IDS
Hostname	IPS-5545Xa & b	IDS-4300
IP address	10.4.24.27 & .28	10.4.32.171
Network mask	255.255.255.224	255.255.255.192
Default gateway	10.4.24.1	10.4.32.129
Location	Internet edge distribution switch	WAN aggregation distribution switch

Process

Deploying IPS

1. Configure LAN switch access port
2. Initialize the IPS module
3. Complete the initial setup
4. Finish the basic configuration
5. Modify the inline security policy

Procedure 1

Configure LAN switch access port

A LAN switch near the IPS sensor provides connectivity for the sensor's management interface. On the Cisco ASA 5500-X Series firewalls, the firewall and IPS modules share a single management interface. This deployment uses the management interface for IPS module access only and the management interface is not used for the firewall.

Step 1: On the appropriate switch to which the IPS device's management port will be connected, configure an access port to the management VLAN.

```
interface GigabitEthernet1/0/19
  description IPS-5545Xa
  switchport
  switchport access vlan 300
  switchport mode access
  spanning-tree portfast
```


Step 2: Configure the LAN distribution switch interfaces that are connected to the Cisco ASA management interfaces. This allows management access to the IPS modules.

```
interface GigabitEthernet1/0/19
  description IPS-5545Xa
!
interface GigabitEthernet2/0/19
  description IPS-5545Xb
!
interface range GigabitEthernet1/0/19, GigabitEthernet2/0/19
  switchport access vlan 300
  switchport mode access
  spanning-tree portfast
```



Tech Tip

The IPS module and Cisco ASA share the same physical port for management traffic. In this deployment, Cisco ASA is managed in-band, and the IPS, either module or appliance, is always managed from the dedicated management port.

Procedure 2

Initialize the IPS module

When a Cisco ASA 5500 Series IPS Solution module is initially deployed, the software IPS module may not be initialized, resulting in the Cisco ASA firewall being unaware of what code version to boot for the IPS module. This procedure verifies the IPS module status and prepares for configuration completion.

Step 1: From the Cisco ASA command line interface, run the following command.

```
IE-ASA5545X# show module ips detail
```

Step 2: If the status shown below is **Up**, then the IPS module software has been loaded and you can skip to Procedure 3.

```
IE-ASA5545X# show module ips detail
```

Getting details from the Service Module, please wait...

```
Card Type:          ASA 5545-X IPS Security Services Processor
Model:             ASA5545-IPS
Hardware version:  N/A
Serial Number:     FCH161170MA
Firmware version:  N/A
Software version:  7.1(6)E4
MAC Address Range: c464.1339.a354 to c464.1339.a354
App. name:         IPS
App. Status:       Up
App. Status Desc:  Normal Operation
App. version:      7.1(6)E4
Data Plane Status: Up
```

Status: Up

If the status shown is **Status: Unresponsive No Image Present**, then the IPS module software has never been loaded. Continue to the next step.

```
IE-ASA5545X# show module ips detail
```

Getting details from the Service Module, please wait...

Unable to read details from module ips

```
Card Type:          Unknown
Model:             N/A
Hardware version:  N/A
Serial Number:     FCH16097J3F
Firmware version:  N/A
Software version:  N/A
MAC Address Range: c464.1339.2cf1 to c464.1339.2cf1
Data Plane Status: Not Applicable
```

Status: Unresponsive No Image Present

...

Step 3: Verify you have the correct IPS image on the Cisco ASA firewall disk0:

i Tech Tip

IPS recovery requires an image with file extension .aip
 IPS upgrades require an image with file extension .pkg
 The two image types are incompatible, and the correct type must be used for each type of operation.

```
IE-ASA5545X# dir
Directory of disk0:/
153  -rwx  36827136   14:53:34 Oct 29 2012  asa901-smp-k8.
bin
175  -rwx  17743320   11:12:33 Oct 31 2012  asdm-702.bin
161  -rwx  45854720   11:30:16 Sep 19 2012  IPS-SSP_5545-
K9-sys-1.1-a-7.1-6-E4.aip
```

Step 4: Configure the IPS module to load the recovery software on disk0, and then boot with that software.

```
IE-ASA5545X# sw-module module ips recover configure image
disk0:/IPS-SSP_5545-K9-sys-1.1-a-7.1-6-E4.aip
IE-ASA5545X# sw-module module ips recover boot
```

Module ips will be recovered. This may erase all configuration and all data on that device and attempt to download/install a new image for it. This may take several minutes.

```
Recover module ips? [confirm]y
Recover issued for module ips.
```

Step 5: After a few minutes, run the following command, and then verify that the module status is Up.

```
IE-ASA5545X# show module ips detail
```

Procedure 3

Complete the initial setup

The initial setup will involve configuring each IPS device (module or appliance) with the initial networking information in order to allow the use of the GUI to complete the configuration.

Table 7 - IPS device configuration

Device characteristics	Internet Edge IPS	Distribution IDS
Device Type	Software module	Appliance
Hostname	IPS-5545Xa & b	IDS-4300
IP address	10.4.24.27 & .28	10.4.32.171
Network mask	255.255.255.224	255.255.255.192
Default gateway	10.4.24.1	10.4.32.129
Location	Internet Edge distribution switch	WAN aggregation distribution switch

Step 1: If you are using Cisco ASA 5545-X, log into the Cisco ASA appliance, and then access the IPS module.

```
IE-ASA5545X# session ips
Opening command session with module ips.
Connected to module ips. Escape character sequence is 'CTRL-
^X'.
```

If you are using a Cisco IPS 4300 or 4500 Series appliance, open a CLI session on the sensor's console port.



Tech Tip

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 2: Run the **setup** command for either the module or an IPS appliance to start the System Configuration Dialog.

```
sensor# setup
Enter host name[sensor]: IPS-5545Xa
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: 10.4.48.0/24
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
```

```
...
```

```
--- Configuration Saved ---
```

Complete the advanced setup using CLI or IDM.

To use IDM, point your web browser at `https://<sensor-ip-address>`.

Step 3: Enter the escape sequence **Ctrl-Shift-6 X**. The Cisco ASA command line returns.

Step 4: Repeat Step 2 for the IPS module in the standby Cisco ASA appliance or for the IPS appliance being deployed in IDS mode on a distribution switch.



Tech Tip

A different host name and IP address must be used on each IPS device so that monitoring systems do not get confused. In this example, IPS-5545Xb and 10.4.24.28 were used on the standby Cisco ASA 5500 Series IPS Solution module.

Procedure 4

Finish the basic configuration

Once the basic setup in the System Configuration Dialog is complete, you will use the startup wizard in the integrated management tool, Cisco Adaptive Security Device Manager/IPS Device Manager (ASDM/IDM) for Cisco ASAs, or Cisco IDM for Cisco IPS Sensor appliances, in order to complete the remaining IPS configuration tasks:

- Configure time settings
- Configure DNS and NTP servers
- Define a basic IPS configuration
- Configure Inspection Service Rule Policy
- Assign interfaces to virtual sensors

This procedure offers two options. If you are configuring IPS modules in

Cisco ASA appliances, complete Option 1. If you are configuring IPS appliances, complete Option 2.

Option 1. Complete the basic configuration for Cisco ASA IPS modules

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://10.4.24.30>)

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

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

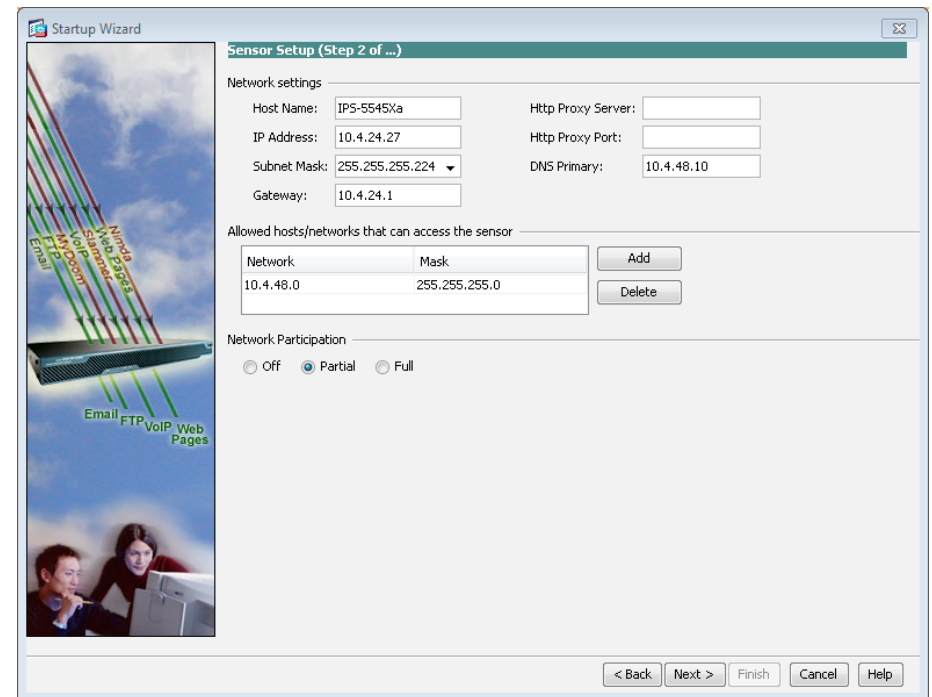
Cisco ASDM imports the current configuration from the IPS sensor, and the startup wizard launcher is displayed in the main window.

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

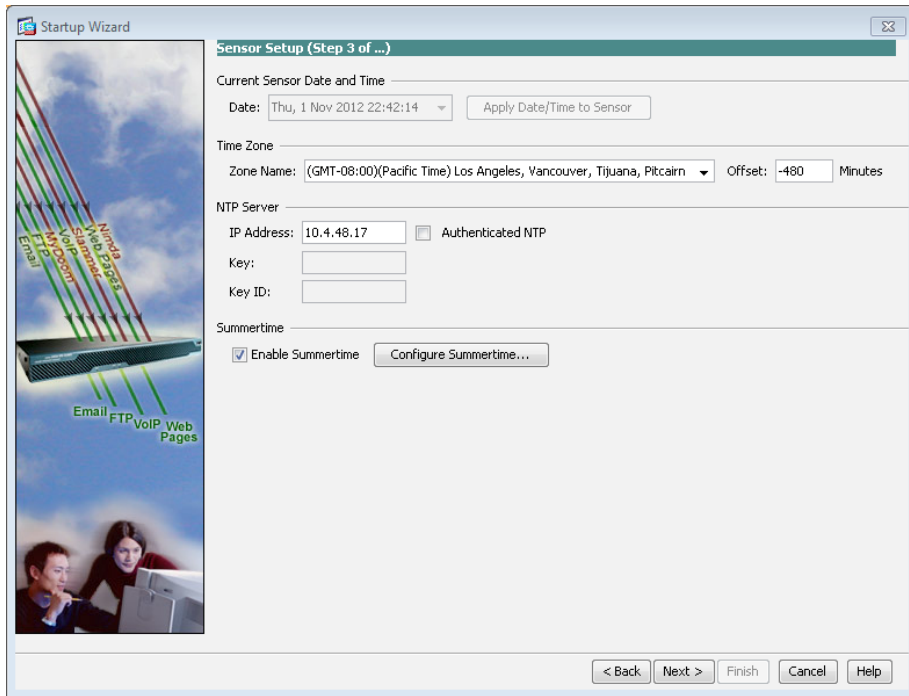


Step 5: Follow the instructions in the wizard. Note the following:

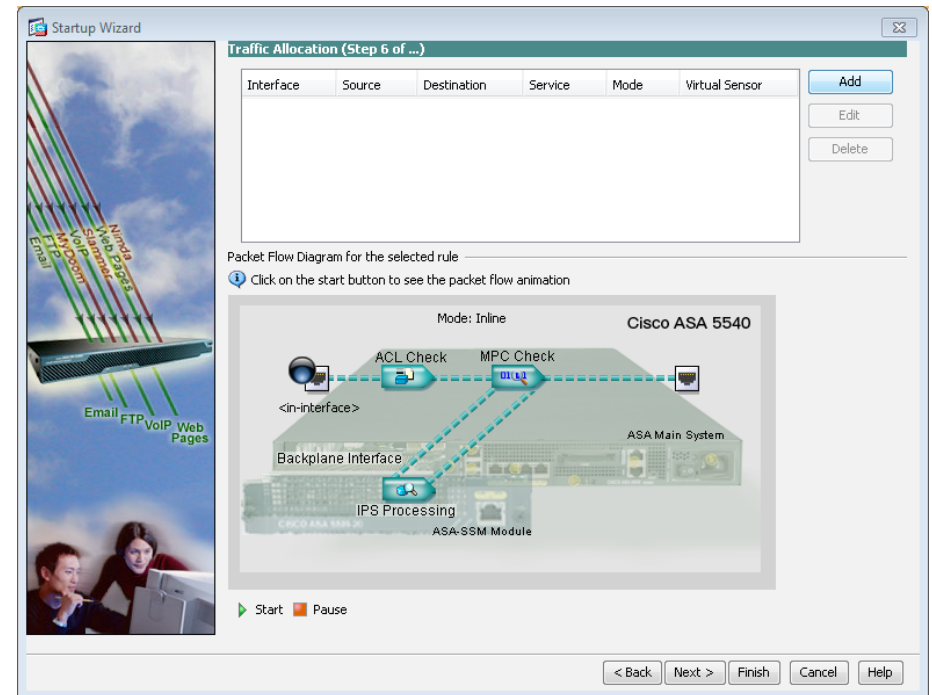
- On the Sensor Setup page, verify the settings, and then click **Next**.



- On the next Sensor Setup page, in the **Zone Name** list, select the appropriate time zone. Enter the NTP Server IP address (Ex: 10.4.48.17), ensure that **Authenticated NTP** is clear, set the summertime settings, and then click **Next**.

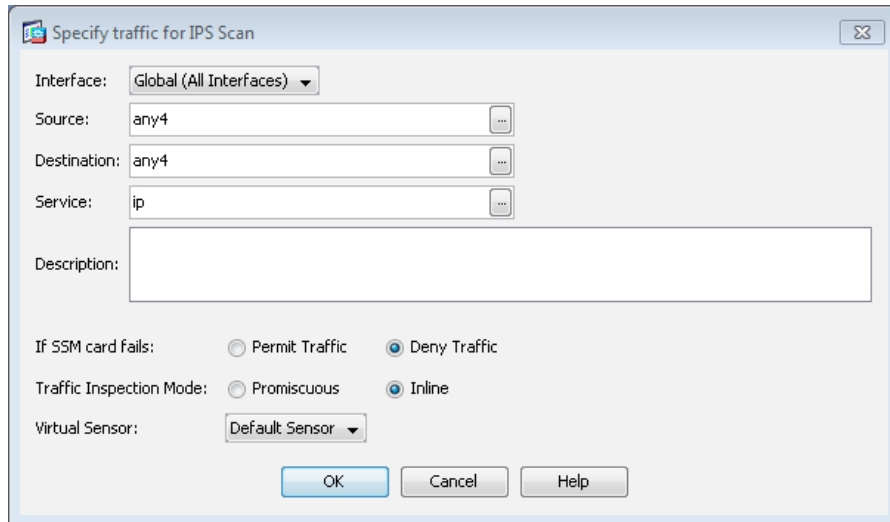


- On the Traffic Allocation page, click **Add**.

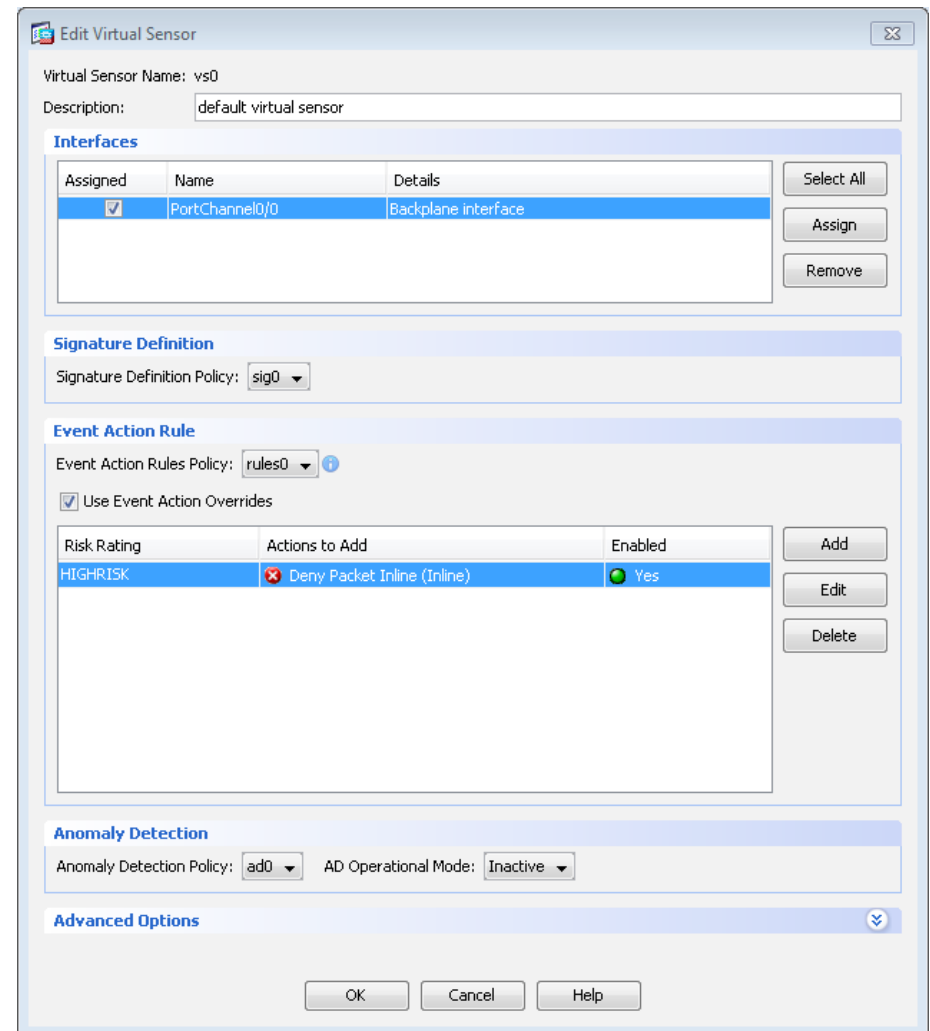


If Cisco ASA already had a default traffic allocation policy, a “The Service Rule Policy you are trying to create already exists” message appears. If you receive this message, click **Cancel**, and then on the Traffic Allocation page, click **Next**.

If the Specify traffic for IPS Scan dialog box appears, under **Traffic Inspection Mode**, select **Inline**, and then click **OK**. On the Traffic Allocation page, click **Next**.



Step 10: In the Edit Virtual Sensor dialog box, for the PortChannel0/0 interface, select **Assigned**, and then click **OK**.



- On the Auto Update page, you configure the IPS device to automatically pull updates from Cisco.com. Select **Enable Signature and Engine Updates**. Provide a valid cisco.com username and password that holds entitlement to download IPS software updates. Select **Daily**, enter a time between 12:00 AM and 4:00 AM for the update **Start Time**, and then select **Every Day**. Click **Finish**

Step 6: When you are prompted if you want to commit your changes to the sensor, click **Yes**. ASDM/IDM applies your changes and a dialog box indicates that a reboot is required.

Step 7: Click **OK**. Do not reboot the IPS sensor yet. Next, you will assign interfaces to the virtual sensor.

Step 8: Navigate to **Sensor Setup > Policies > IPS Policies**.

Step 9: Highlight the vs0 virtual sensor, and then click **Edit**.

Step 11: Click Apply.

Configuration > IPS > Policies > IPS Policies

+ Add Virtual Sensor Edit Delete

Name	Assigned Interfaces (or Pairs)	Signature Definition Policy	Event Action Override Policy	Anomaly Detection Policy	Description
vs0	PortChannel0/0.0 (Backplane Interface)	sig0	rules0 (1 action overrides) HIGHRISK Deny Packet Initi... Yes	ad0	default virtual se...

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

Event Action Filters IPv4 Target Value Rating IPv6 Target Value Rating OS Identifications Event Variables Risk Category Threat Category General

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

+ Add Edit Delete

Name	Enabled	Sig ID	SubSig ID	Attacker (IPv4 / IPv6 / port)	(IPv4 /
------	---------	--------	-----------	-------------------------------	---------

Apply Reset

Next, you will reboot the sensor.

Step 12: Navigate to Sensor Management > Reboot Sensor.

Step 13: Click **Reboot Sensor**, in the Reboot Sensor dialog box, and then click **OK**.

Reboot Sensor

Step 14: Repeat the steps in Option 1 for the IPS module in the resilient Cisco ASA firewall. There is no configuration synchronization between the two IPS modules like there is between the Cisco ASA firewalls. Note that in Step 1, from a client on the internal network, navigate to the resilient firewalls inside IP address, and then launch Cisco ASDM. (Example: <https://10.4.24.29>)



Tech Tip

Do not attempt to modify the firewall configuration on the standby Cisco ASA. Configuration changes are only made on the primary Cisco ASA.

Option 2. Complete the basic configuration for Cisco IPS 4300 or 4500 Series Sensor appliance

Step 1: Configure the distribution switch.

If a VLAN does not already exist on the distribution layer switch, configure it now.

```
vlan 350
 name WAN_Service_Net
```

Step 2: If necessary, configure Layer 3.

Be sure to configure a VLAN interface (SVI) for every new VLAN you add, so devices in the VLAN can communicate with the rest of the network.

```
interface Vlan350
 ip address 10.4.32.129 255.255.255.192
 no shutdown
```

Step 3: On the distribution switch to which the sensor's management ports are connected, in a command-line interface, connect the IPS management interface to the distribution switch.

```
interface GigabitEthernet1/0/5
 description IPS4345 management port
 switchport access vlan 350
 switchport mode access
 spanning-tree portfast
 no shutdown
```

Step 4: On the distribution switch to which the sensor's monitoring ports are connected, in a command-line interface, select the source interfaces that the IPS system will monitor and select the destination interfaces that receive copies of the monitored traffic.



Tech Tip

It is possible to oversubscribe the destination interfaces used with the monitor session feature. Monitor the output rate of the destination interface in order to determine if the interface is close to its limit.

```
interface GigabitEthernet1/0/24
description IPS4345 G0/0
no switchport
no ip address
no shutdown
```

```
interface GigabitEthernet2/0/24
description IPS4345 G0/1
no switchport
no ip address
no shutdown
```

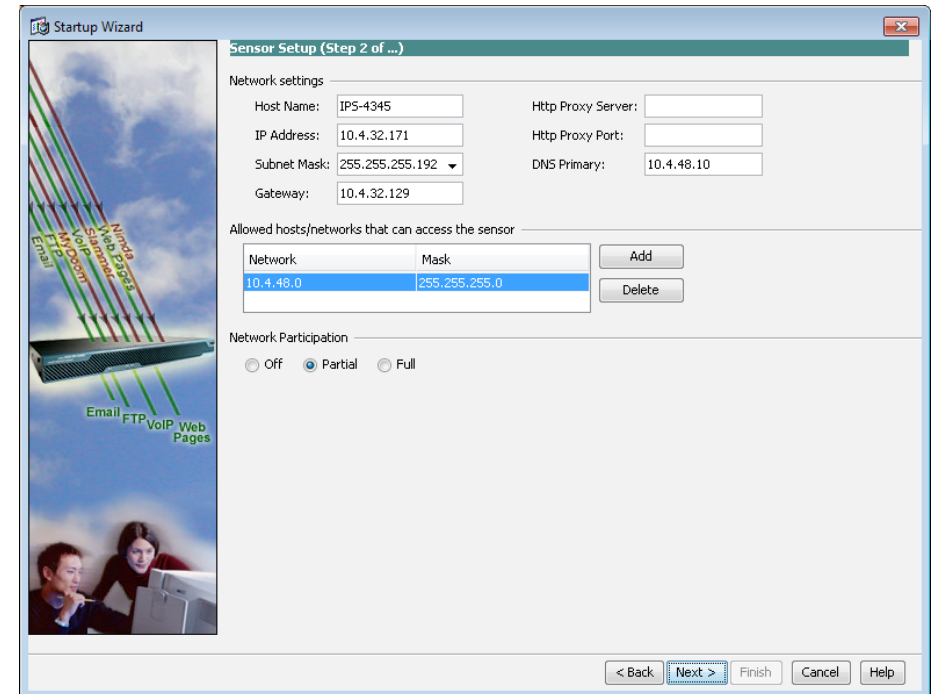
```
monitor session 1 source interface TenGigabitEthernet1/1/1, TenGigabitEthernet2/1/1 both
monitor session 1 destination interface GigabitEthernet1/0/24, GigabitEthernet2/0/24
```

Step 5: HTTPS to the management IP address on the Cisco IPS appliance (Example: <https://10.4.32.171>) to launch IDM.

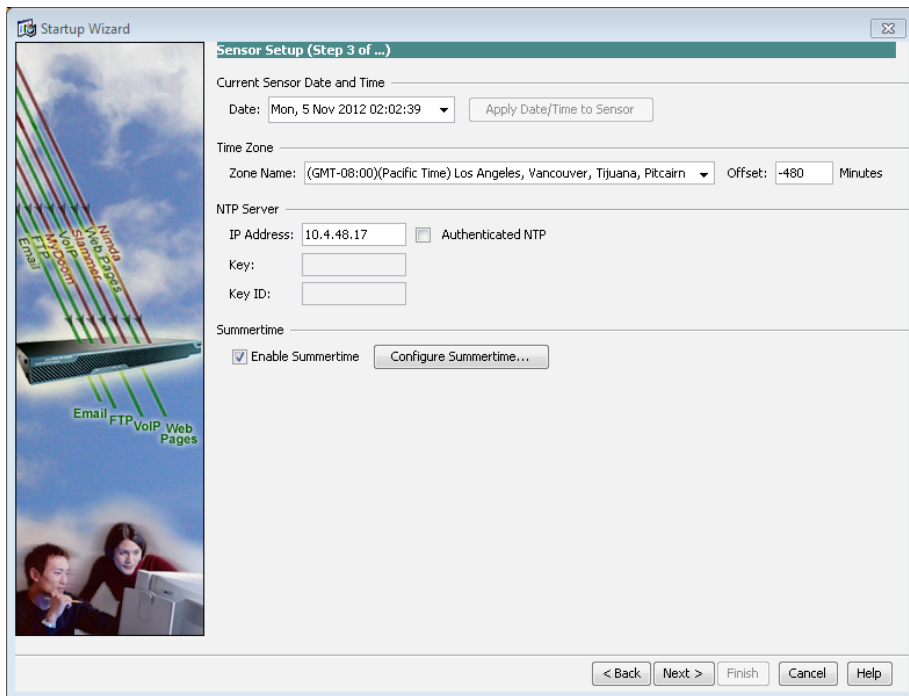
Step 6: Navigate to **Configuration > Sensor Setup > Startup Wizard**, and then click **Launch Startup Wizard**.

Step 7: Follow the instructions in the wizard. Note the following:

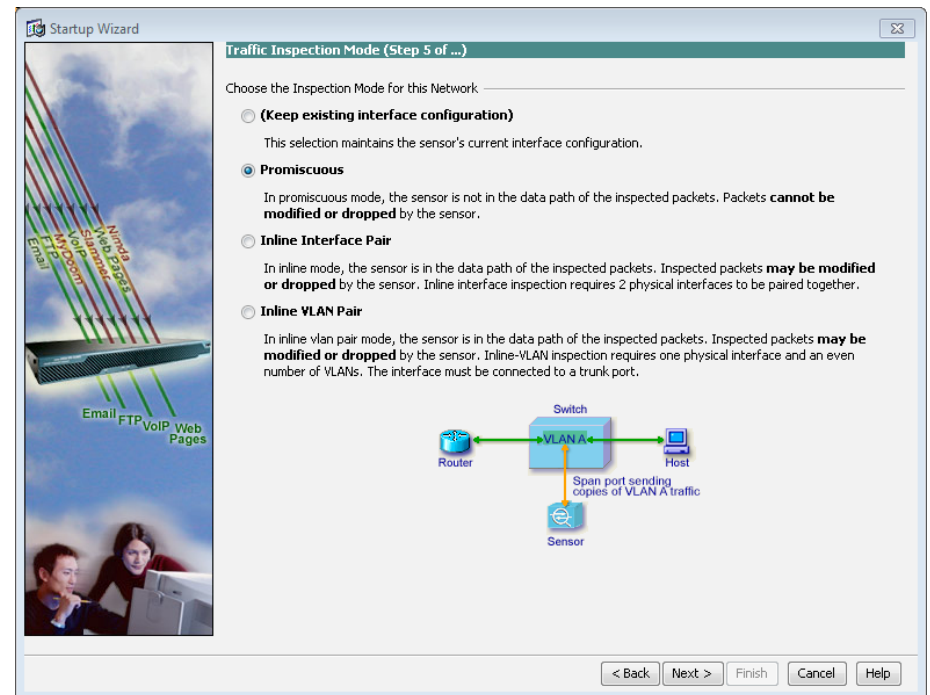
- On the Sensor Setup page, verify the settings, and then click **Next**.



- On the next **Sensor Setup** page, in the **Zone Name** list, select the appropriate time zone. Enter the NTP Server IP address (Ex: 10.4.48.17), ensure that **Authenticated NTP** is clear, set the summertime settings, and then click **Next**.



- On the Traffic Inspection Mode page, select **Promiscuous**, and then click **Next**.



- On the Interface Selection page, in the **Select Interface** list, select **GigabitEthernet0/0**, and then click **Next**.
- On the Virtual Sensors page, review the configuration, and then click **Next**.
- On the Auto Update page, you configure the IPS device to automatically pull updates from Cisco.com. Select **Enable Signature and Engine Updates**. Provide a valid cisco.com username and password that holds entitlement to download IPS software updates. Select **Daily**, enter a time between 12:00 AM and 4:00 AM for the update **Start Time**, and then select **Every Day**. Click **Finish**.

Step 8: When you are prompted if you want to commit your changes to the sensor, click **Yes**. IDM applies your changes and replies with an indication that a reboot is required.

Step 9: Click **OK**. Do not reboot the IPS sensor yet.

Because the appliance has multiple physical interfaces, more than one can be used to inspect traffic (either in inline or promiscuous mode). In this deployment, you will assign an additional interface on the appliance to be used for promiscuous mode as a resilient interface on the other switch in the switch stack.

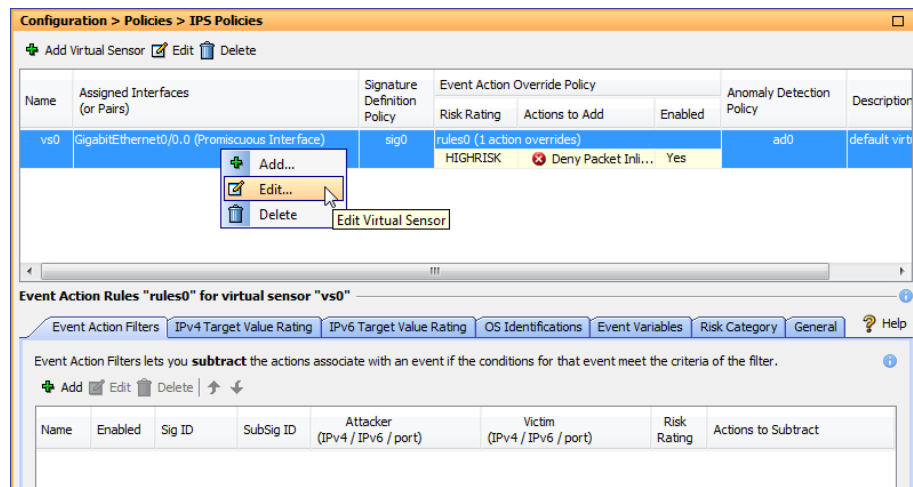
Step 10: In the IPS configuration pane of IDM, navigate to **Configuration > Interfaces > Interfaces**.

Step 11: Select interface **GigabitEthernet 0/1**, and then click **Enable**.

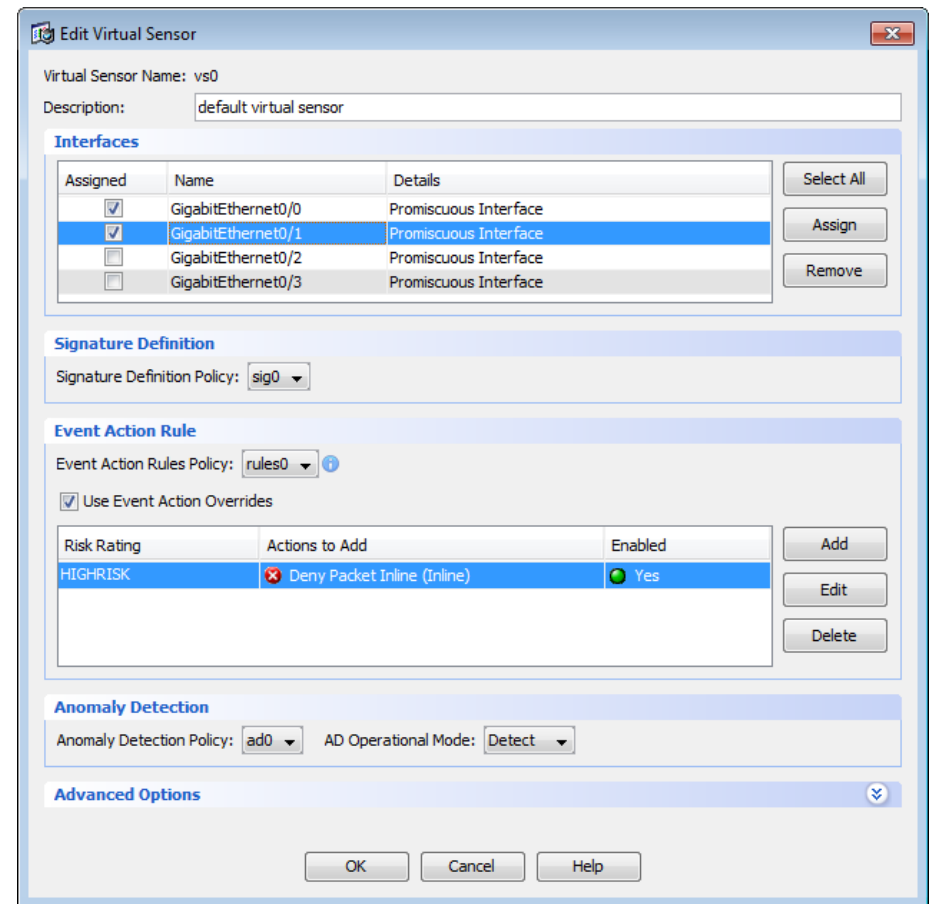
Step 12: Click **Apply** and then click **OK**.

Step 13: Navigate to **Configuration > Policies > IPS Policies**.

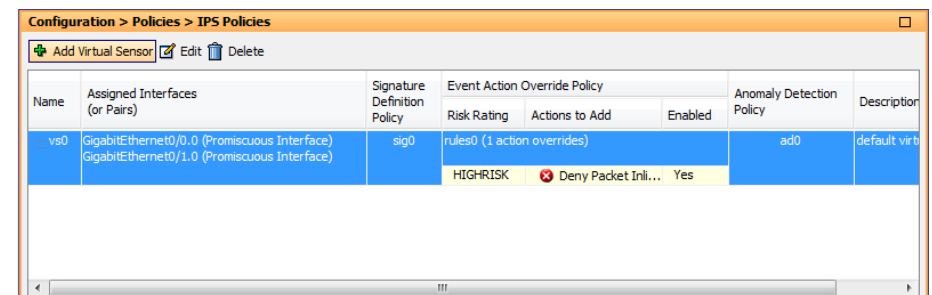
Step 14: Right-click **vs0**, and then select **Edit**.



Step 15: In the Edit Virtual Sensor dialog box, for **GigabitEthernet0/1**, select the **Assigned** box, and then click **OK**.



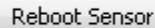
Step 16: Click **Apply**.



Next, you will reboot the sensor.

Step 17: Navigate to **Sensor Management > Reboot Sensor**.

Step 18: Click **Reboot Sensor**. In the Reboot Sensor dialog box, click **OK**.



Procedure 5 Modify the inline security policy

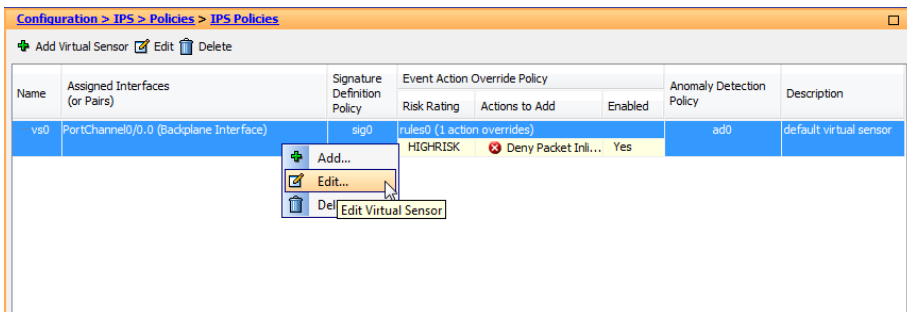
(Optional)

If you opted to run inline mode on an IPS device, 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: In Cisco ASDM/IDM, navigate to **Configuration > IPS > Policies > IPS Policies**.

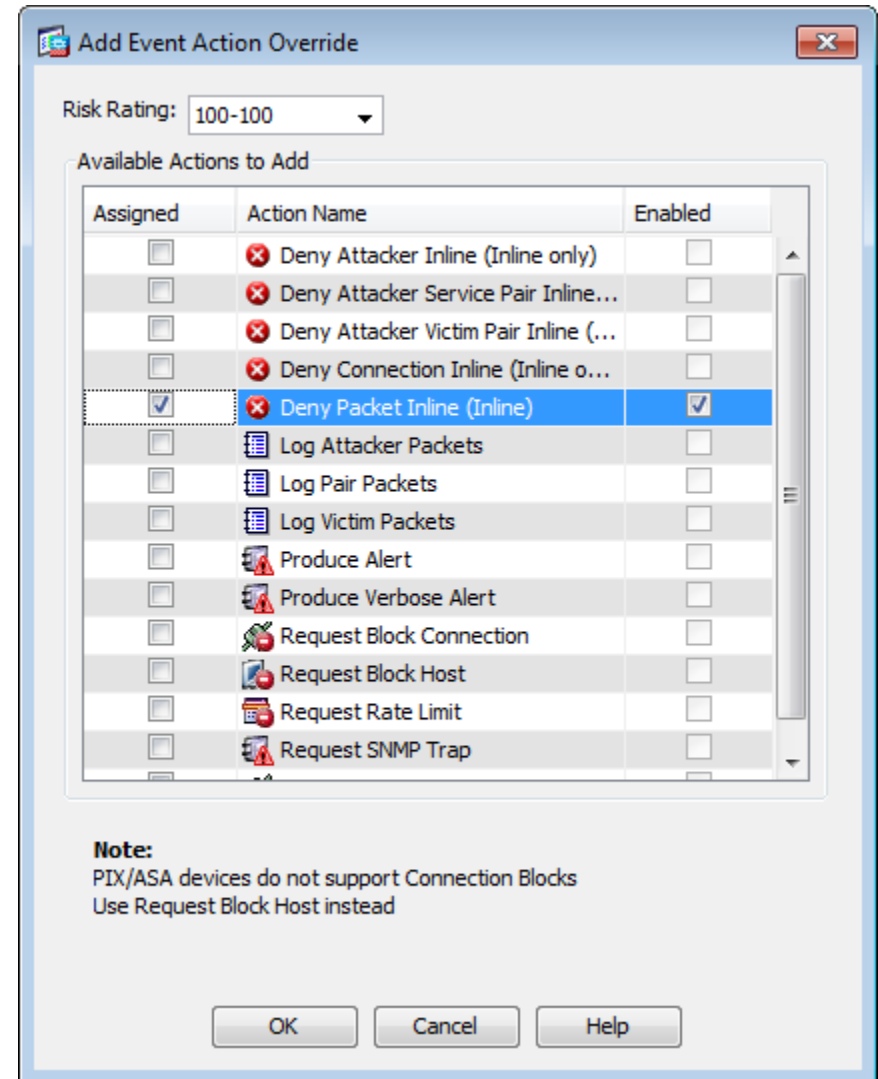
Step 2: In the Virtual Sensor panel, right-click the **vs0** entry, and then select **Edit**.



Step 3: In the Event Action Rule work pane, click **Deny Packet Inline Override**, and then click **Delete**.

Step 4: In the Event Action Rule work pane, Click **Add**.

Step 5: In the Add Event Action Override dialog box, in the **Risk Rating** list, enter **100-100**, select **Deny Packet Inline**, and then click **OK**.



Step 6: Click **Apply**.

Step 7: If you have additional IPS devices, repeat Step 1 through Step 7 for each device.

Intrusion Prevention Summary

Organizations are exposed to a large number of threats from the Internet. Cisco IPS deployed in the Internet edge of an organization or internally plays a significant role in identifying and blocking malicious traffic, and it improves the availability and security of the Internet-facing services as well as helping to identify issues and problems occurring on the LAN.

Notes

Appendix A: Product List

Internet Edge

Functional Area	Product Description	Part Numbers	Software
Firewall	Cisco ASA 5545-X IPS Edition - security appliance	ASA5545-IPS-K9	ASA 9.0(1) IPS 7.1(6)E4
	Cisco ASA 5525-X IPS Edition - security appliance	ASA5525-IPS-K9	
	Cisco ASA 5515-X IPS Edition - security appliance	ASA5515-IPS-K9	
	Cisco ASA 5512-X IPS Edition - security appliance	ASA5512-IPS-K9	
	Cisco ASA5512-X Security Plus license	ASA5512-SEC-PL	
	Firewall Management	ASDM	7.0(2)

Internet Edge LAN

Functional Area	Product Description	Part Numbers	Software
DMZ Switch	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 ports	WS-C3750X-24T-S	15.0(2)SE IP Base License
Outside Switch	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 ports and Four GbE SFP Uplink ports	WS-C2960S-24TS-L	15.0(1)SE2 LAN Base License

IPS

Functional Area	Product Description	Part Numbers	Software
Distribution IDS	Cisco IPS 4520	IPS-4520-K9	7.1(6)E4
	Cisco IPS 4510	IPS-4510-K9	
	Cisco IPS 4360	IPS-4360-K9	
	Cisco IPS 4345	IPS-4345-K9	

LAN Distribution Layer

Functional Area	Product Description	Part Numbers	Software
Modular Distribution Layer Virtual Switch Pair	Cisco Catalyst 6500 E-Series 6-Slot Chassis	WS-C6506-E	15.0(1)SY1 IP Services License
	Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4	VS-S2T-10G	
	Cisco Catalyst 6500 16-port 10GbE Fiber Module w/DFC4	WS-X6816-10G-2T	
	Cisco Catalyst 6500 24-port GbE SFP Fiber Module w/DFC4	WS-X6824-SFP-2T	
	Cisco Catalyst 6500 4-port 40GbE/16-port 10GbE Fiber Module w/DFC4	WS-X6904-40G-2T	
	Cisco Catalyst 6500 4-port 10GbE SFP+ adapter for WX-X6904-40G module	CVR-CFP-4SFP10G	
Modular Distribution Layer Switch	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.3.0.SG(15.1-1SG) Enterprise Services License
	Cisco Catalyst 4500 E-Series Supervisor Engine 7-E, 848Gbps	WS-X45-SUP7-E	
	Cisco Catalyst 4500 E-Series 24-port GbE SFP Fiber Module	WS-X4624-SFP-E	
	Cisco Catalyst 4500 E-Series 12-port 10GbE SFP+ Fiber Module	WS-X4712-SFP+E	
Stackable Distribution Layer Switch	Cisco Catalyst 3750-X Series Stackable 12 GbE SFP ports	WS-C3750X-12S-E	15.0(2)SE IP Services License
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	

Appendix B: Configuration Example

ASA Firewall 5545X

```
ASA Version 9.0(1)
!
hostname IE-ASA5545X
domain-name cisco.local
enable password 8Ry2YjIyt7RRXU24 encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0/0
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/0.300
 vlan 300
 nameif inside
 security-level 100
 ip address 10.4.24.30 255.255.255.224 standby 10.4.24.29
 summary-address eigrp 100 10.4.28.0 255.255.252.0 5
!
interface GigabitEthernet0/1
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/1.1116
 description Web Server connection on VLAN 116
 vlan 1116
 nameif dmz-web
 security-level 50
 ip address 192.168.16.1 255.255.255.0 standby 192.168.16.2
 ipv6 address 2001:db8:a:1::1/64 standby 2001:db8:a:1::2
 ipv6 enable
!
interface GigabitEthernet0/1.1123
 vlan 1123
 nameif dmz-management
 security-level 50
 ip address 192.168.23.1 255.255.255.0 standby 192.168.23.2
!
interface GigabitEthernet0/2
 description LAN/STATE Failover Interface
!
interface GigabitEthernet0/3
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3.16
 description Primary Internet connection on VLAN 16
 vlan 16
 nameif outside-16
 security-level 0
 ip address 172.16.130.124 255.255.255.0 standby 172.16.130.123
```

```

!
interface GigabitEthernet0/3.17
  description Resilient Internet connection on VLAN 17
  vlan 17
  nameif outside-17
  security-level 0
  ip address 172.17.130.124 255.255.255.0 standby 172.17.130.123
!
interface GigabitEthernet0/4
  shutdown
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet0/5
  shutdown
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet0/6
  shutdown
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet0/7
  shutdown
  no nameif
  no security-level
  no ip address
!
interface Management0/0
  management-only
  nameif IPS-mgmt
  security-level 0
  no ip address

```

```

!
boot system disk0:/asa901-smp-k8.bin
ftp mode passive
clock timezone PST -8
clock summer-time PDT recurring
dns domain-lookup inside
dns server-group DefaultDNS
  name-server 10.4.48.10
  domain-name cisco.local
same-security-traffic permit intra-interface
object network internal-network
  subnet 10.4.0.0 255.254.0.0
  description The organization's internal network range
object network dmz-networks
  subnet 192.168.16.0 255.255.248.0
  description The organization's DMZ network range
object network internal-network-ISPa
  subnet 10.4.0.0 255.254.0.0
  description PAT traffic from inside out the primary Internet
connection
object network internal-network-ISPb
  subnet 10.4.0.0 255.254.0.0
  description PAT traffic from inside out the secondary internet
connection
object network outside-webserver-ISPa
  host 172.16.130.100
  description WebServer on ISP A
object network dmz-webserver-ISPa
  host 192.168.16.100
object network outside-webserver-ISPb
  host 172.17.130.100
  description WebServer on ISPb
object network dmz-webserver-ISPb
  host 192.168.16.100
  description NAT the webserver in the DMZ to outside address on
ISP B
object network dmz-dmvpn-1

```



```

host 192.168.18.10
description NAT the primary DMVPN hub router in the DMZ to ISP A
object network dmz-dmvpn-2
host 192.168.18.11
description NAT the secondary DMVPN hub router in the DMZ to ISP
B
object network outside-dmvpn-ISPa
host 172.16.130.1
description DMVPN hub router on ISP A
object network outside-dmvpn-ISPB
host 172.17.130.1
description DMVPN hub router on ISP B

object network dmz-guest-network-ISPa
subnet 192.168.28.0 255.255.252.0
description DMZ outside PAT addresses for ISPa
object network internal-aaa
host 10.4.48.15
description Internal AAA Server
object network internal-ntp
host 10.4.48.17
description Internal NTP Server
object network internal-dhcp
host 10.4.48.10
description Internal DHCP Server
object network internal-dns
host 10.4.48.10
description Internal DNS Server
object-group service DM_INLINE_TCP_1 tcp
port-object eq www
port-object eq https
object-group service DM_INLINE_TCP_2 tcp
port-object eq www
port-object eq https
object-group service DM_INLINE_TCP_3 tcp
port-object eq www

```

```

port-object eq https
object-group service DM_INLINE_SERVICE_4
service-object tcp destination eq tacacs
service-object udp destination eq 1812
service-object udp destination eq 1813
object-group service DM_INLINE_SERVICE_6
service-object tcp destination eq domain
service-object udp destination eq domain
object-group network DM_INLINE_NETWORK_1
network-object object dmz-networks
network-object object internal-network
object-group service DM_INLINE_TCP_5 tcp
port-object eq www
port-object eq https

object-group service DM_INLINE_UDP_1 udp
port-object eq 1812
port-object eq 1813
object-group service DM_INLINE_TCP_6 tcp
port-object eq www
port-object eq https
object-group service DM_INLINE_TCP_7 tcp
port-object eq www
port-object eq https
object-group service DM_INLINE_SERVICE_7
service-object tcp destination eq 135
service-object tcp destination eq 445
service-object tcp destination eq kerberos
service-object tcp destination eq ldap
service-object udp destination eq 389
service-object udp destination eq ntp
object-group service DM_INLINE_TCP_8 tcp
port-object eq www
port-object eq https
access-list global_access remark Permit management protocols from
the management DMZ to the internal network
access-list global_access extended permit object-group DM_INLINE_

```

```

SERVICE_1 192.168.23.0 255.255.255.0 object internal-network
access-list global_access remark Allow anyone to access the
webservers in the DMZ
access-list global_access extended permit tcp any 192.168.16.0
255.255.255.0 object-group DM_INLINE_TCP_1
access-list global_access extended permit icmp any 192.168.18.0
255.255.255.0 object-group DM_INLINE_ICMP_1
access-list global_access extended permit object-group DM_INLINE
SERVICE_3 any object dmz-dmvpn-2
access-list global_access remark Allow traffic to the DMVPN hub
routers
access-list global_access extended permit object-group DM_INLINE
SERVICE_2 any object dmz-dmvpn-1
access-list global_access remark Allow WLC's to communicate with
the NTP server locate din the data center.
access-list global_access extended permit udp object-group dmz-
wlc-group object internal-ntp eq ntp
access-list global_access remark Allow DMZ based WLC's to
communicate with the AAA/ACS Server on the internal network.
access-list global_access extended permit object-group DM_INLINE
SERVICE_4 object-group dmz-wlc-group object internal-aaa
access-list global_access extended permit tcp object-group dmz-
wlc-group any object-group DM_INLINE_TCP_4
access-list global_access remark Allow DMZ based WLC's to
communicate with the internal WLC's
access-list global_access extended permit object-group DM_INLINE
SERVICE_5 object-group dmz-wlc-group object-group internal-wlc-
group
access-list global_access remark Allow DMZ WLC's to obtain IP
address via internal DHCP server
access-list global_access extended permit udp object-group dmz-
wlc-group object internal-dhcp eq bootps
access-list global_access remark Allow wireless guest users to
obtain an IP address from the internal DHCP server.
access-list global_access extended permit udp 192.168.28.0
255.255.252.0 object internal-dhcp eq bootps
access-list global_access remark Allow Guest Wireless Users to

```

```

resolve DNS names.
access-list global_access extended permit object-group DM_INLINE
SERVICE_6 192.168.28.0 255.255.252.0 object internal-dns
access-list global_access remark Allow wireless guest users
access to the DMZ based webservers, possibly for walled garden
access
access-list global_access extended permit tcp 192.168.28.0
255.255.252.0 192.168.16.0 255.255.255.0 object-group DM_INLINE
TCP_5
access-list global_access remark Allow Standby AP-SSO WLC's to
communicate to internal NTP server using RP Port
access-list global_access extended permit udp object-group dmz-
wlc-RP-group object internal-ntp eq ntp
access-list global_access remark Allow ELC to connect to ISE
access-list global_access extended permit udp 192.168.19.0
255.255.255.0 object internal_ISE-1 object-group DM_INLINE_UDP_1
access-list global_access remark guest client web auth access to
ISE
access-list global_access extended permit tcp 192.168.28.0
255.255.252.0 object internal_ISE-1 eq 8443
access-list global_access remark Deny traffic from the wireless
guest network to the internal and dmz resources
access-list global_access extended deny ip 192.168.28.0
255.255.252.0 object-group DM_INLINE_NETWORK_1
access-list global_access remark Allow Wireless DMZ users access
to the internet
access-list global_access extended permit ip 192.168.28.0
255.255.252.0 any
access-list global_access remark Exchange to ESA outbound SMTP
access-list global_access extended permit tcp object internal-
exchange 192.168.17.0 255.255.255.0 eq smtp
access-list global_access remark Block other outbound SMTP
access-list global_access extended deny tcp object internal-
network any4 eq smtp
access-list global_access remark Internet to ESA inbound SMTP
access-list global_access extended permit tcp any4 192.168.17.0
255.255.255.0 eq smtp

```

```

access-list global_access remark ESA to Exchange inbound SMTP
access-list global_access extended permit tcp 192.168.17.0
255.255.255.0 object internal-exchange eq smtp
access-list global_access remark DNS
access-list global_access extended permit udp 192.168.17.0
255.255.255.0 object internal-dns eq domain
access-list global_access remark NTP
access-list global_access extended permit udp 192.168.17.0
255.255.255.0 object internal-ntp eq ntp
access-list global_access remark Block other to internal networks
access-list global_access extended deny ip 192.168.17.0
255.255.255.0 object internal-network
access-list global_access remark ESA to internet outbound SMTP
access-list global_access extended permit tcp 192.168.17.0
255.255.255.0 any4 eq smtp
access-list global_access remark HTTP to Internet
access-list global_access extended permit tcp 192.168.17.0
255.255.255.0 any4 eq www
access-list global_access remark HTTPS to Internet
access-list global_access extended permit tcp 192.168.17.0
255.255.255.0 any4 eq https
access-list global_access remark Deny IP traffic from the DMZ to
any other network
access-list global_access extended deny ip object dmz-networks
any4
access-list global_access extended deny tcp object internal-
network any4 eq telnet
access-list global_access extended permit ip object internal-
network any4 log disable
access-list global_access extended permit tcp any6 object dmz-
web-net-v6 object-group DM_INLINE_TCP_2
access-list global_access extended permit tcp any6 object dmz-
webserver-ispv6 object-group DM_INLINE_TCP_3
access-list global_access remark Permint HTTP/HTTPS traffic onto
the TMG DMZ
access-list global_access extended permit tcp any4 192.168.22.0
255.255.255.0 object-group DM_INLINE_TCP_6

```

```

access-list global_access remark Permit HTTP/HTTPS from TMG to
the internal Exchange Server
access-list global_access extended permit tcp 192.168.22.0
255.255.255.0 object internal-exchange object-group DM_INLINE
TCP_7 log disable
access-list global_access remark Internal DNS
access-list global_access extended permit udp 192.168.22.0
255.255.255.0 object internal-dns eq domain
access-list global_access remark TMG Server requires HTTP/HTTPS
to get to the internet for updates.
access-list global_access extended permit tcp 192.168.22.0
255.255.255.0 any4 object-group DM_INLINE_TCP_8
access-list global_access extended permit object-group DM_INLINE
SERVICE_7 192.168.22.0 255.255.255.0 object internal-ad
access-list global_mpc extended permit ip any4 any4
access-list global_mpc_1 remark Do not match any to internal
networks
access-list global_mpc_1 extended deny ip any4 object internal-
network
access-list global_mpc_1 remark Do not match any to DMZ networks
access-list global_mpc_1 extended deny ip any4 object dmz-
networks
access-list global_mpc_1 remark Match HTTP to any other networks
access-list global_mpc_1 extended permit tcp any4 any4 eq www
pager lines 24
logging enable
logging buffered informational
logging asdm informational
mtu inside 1500
mtu dmz-web 1500
mtu dmz-management 1500
mtu outside-16 1500
mtu outside-17 1500
mtu IPS-mgmt 1500
failover
failover lan unit primary
failover lan interface failover GigabitEthernet0/2

```

```

failover polltime unit msec 200 holdtime msec 800
failover polltime interface msec 500 holdtime 5
failover key FailoverKey
failover replication http
failover link failover GigabitEthernet0/2
failover interface ip failover 10.4.24.33 255.255.255.248 standby
10.4.24.34
monitor-interface inside
monitor-interface dmz-web
monitor-interface dmz-management
monitor-interface dmz-guests
monitor-interface outside-16
monitor-interface outside-17
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-702.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
!
object network internal-network-ISPa
 nat (any,outside-16) dynamic interface
object network internal-network-ISPb
 nat (any,outside-17) dynamic interface
object network dmz-webserver-ISPa
 nat (any,outside-16) static outside-webserver-ISPa
object network dmz-webserver-ISPb
 nat (any,outside-17) static outside-webserver-ISPb
access-group global_access global
ipv6 route outside-16 ::/0 2001:db8:a::7206
!
router eigrp 100
 no auto-summary
 network 10.4.24.0 255.255.252.0
 network 192.168.16.0 255.255.248.0
 passive-interface default
 no passive-interface inside
 redistribute static

```

```

!
route outside-16 0.0.0.0 0.0.0.0 172.16.130.126 1 track 1
route outside-17 0.0.0.0 0.0.0.0 172.17.130.126 50
route outside-16 172.18.1.1 255.255.255.255 172.16.130.126 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
aaa-server AAA-SERVER protocol tacacs+
aaa-server AAA-SERVER (inside) host 10.4.48.15
 key SecretKey
aaa-server AAA-RADIUS protocol radius
aaa-server AAA-RADIUS (inside) host 10.4.48.15
 key SecretKey
 radius-common-pw SecretKey
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
aaa authorization exec authentication-server
http server enable
http 10.4.48.0 255.255.255.0 inside
http 10.4.63.0 255.255.255.0 inside
snmp-server host inside 10.4.48.35 community cisco
no snmp-server location
no snmp-server contact
snmp-server community cisco
snmp-server enable traps snmp authentication linkup linkdown
coldstart warmstart
sla monitor 16

```

```

type echo protocol ipIcmpEcho 172.18.1.1 interface outside-16
sla monitor schedule 16 life forever start-time now
crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-
md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-
hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-
md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-
hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-
sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-
hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-
sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-
hmac
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map SYSTEM_DEFAULT_CRYPTOMAP 65535 set ikev1
transform-set ESP-AES-128-SHA ESP-AES-128-MD5 ESP-AES-192-SHA
ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-
3DES-MD5 ESP-DES-SHA ESP-DES-MD5
crypto dynamic-map SYSTEM_DEFAULT_CRYPTOMAP 65535 set reverse-
route
crypto map outside-16_map 65535 ipsec-isakmp dynamic SYSTEM_
DEFAULT_CRYPTOMAP
crypto map outside-16_map interface outside-16
crypto ca trustpoint _SmartCallHome_ServerCA
crl configure
crypto ca trustpoint ASDM_TrustPoint0
enrollment self
subject-name CN=IE-ASA5545X
proxy-ldc-issuer
crl configure

```

```

crypto ca trustpool policy
crypto ikev1 enable outside-16
crypto ikev1 policy 10
authentication crack
encryption aes-256
hash sha
group 2
lifetime 86400
crypto ikev1 policy 20
authentication rsa-sig
encryption aes-256
hash sha
group 2
lifetime 86400
crypto ikev1 policy 30
authentication pre-share
encryption aes-256
hash sha
group 2
lifetime 86400
crypto ikev1 policy 40
authentication crack
encryption aes-192
hash sha
group 2
lifetime 86400
crypto ikev1 policy 50
authentication rsa-sig
encryption aes-192
hash sha
group 2
lifetime 86400
crypto ikev1 policy 60
authentication pre-share
encryption aes-192
hash sha
group 2

```

```
lifetime 86400
crypto ikev1 policy 70
 authentication crack
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 80
 authentication rsa-sig
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 90
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 100
 authentication crack
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 110
 authentication rsa-sig
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 120
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
```

```
crypto ikev1 policy 130
 authentication crack
 encryption des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 140
 authentication rsa-sig
 encryption des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 150
 authentication pre-share
 encryption des
 hash sha
 group 2
 lifetime 86400
!
track 1 rtr 16 reachability
telnet timeout 5
ssh 10.4.48.0 255.255.255.0 inside
ssh timeout 5
ssh version 2
console timeout 0
!
tls-proxy maximum-session 1000
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 10.4.48.17
ssl encryption aes256-sha1 aes128-sha1 3des-sha1
!
class-map global-class
 match access-list global_mpc
class-map inspection_default
```

```

match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect ip-options
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
    inspect icmp
  class global-class
    ips inline fail-close
!
service-policy global_policy global
prompt hostname context
: end

```

DMZ Switch 3750X

```

version 15.0
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname DMZ-3750X
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$YN18$x7AuTu0NEYaEbM1oPRkDg1
!
username admin password 7 08221D5D0A16544541
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
  server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
!
!
!
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
switch 1 provision ws-c3750x-24
switch 2 provision ws-c3750x-24
stack-mac persistent timer 0
system mtu routing 1500

```

```

!
!
!
ip domain-name cisco.local
ip name-server 10.4.48.10
vtp mode transparent
udld enable

!
!
!
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1116-1118 priority 24576
!
!
!
port-channel load-balance src-dst-ip
!
vlan internal allocation policy ascending
!
vlan 1116
 name DMZ-WEB
!
vlan 1123
 name DMZ-MANAGEMENT
!
ip ssh version 2
!
!
!
!
macro name AccessEdgeQoS
 auto qos voip cisco-phone

```

```

@
macro name EgressQoS
 mls qos trust dscp
 queue-set 1
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
@
!
!
interface FastEthernet0
 no ip address
 shutdown
!
interface GigabitEthernet1/0/2
 description WEBSERVER
 switchport access vlan 1116
 switchport mode access
 logging event link-status
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust dscp
 macro description EgressQoS
 spanning-tree portfast
!
interface GigabitEthernet1/0/17
 description OUT-2960Sa Fas0
 switchport access vlan 1123
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/24
 description IE-ASA5545Xa Gig0/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1116-1119,1123,1128
 switchport mode trunk
 logging event link-status
 logging event trunk-status

```



```

srr-queue bandwidth share 1 30 35 5

priority-queue out
mls qos trust dscp
macro description EgressQoS | EgressQoS | EgressQoS
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet2/0/2
description WEBSERVER
switchport access vlan 1116
switchport mode access
logging event link-status
srr-queue bandwidth share 1 30 35 5

priority-queue out
mls qos trust dscp
macro description EgressQoS
spanning-tree portfast
!
interface GigabitEthernet2/0/17
description OUT-2960Sb Fas0
switchport access vlan 1123
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet2/0/24
description IE-ASA5545Xb Gig0/1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1116-1119,1123,1128
switchport mode trunk
logging event link-status
logging event trunk-status
srr-queue bandwidth share 1 30 35 5

priority-queue out
mls qos trust dscp

```

```

macro description EgressQoS | EgressQoS | EgressQoS
!
interface Vlan1
no ip address
shutdown
!
interface Vlan1123
description In-band management
ip address 192.168.23.5 255.255.255.0
!
ip default-gateway 192.168.23.1
!
no ip http server
ip http authentication aaa
ip http secure-server
!
!
ip sla enable reaction-alerts
logging esm config
access-list 55 permit 10.4.48.0 0.0.0.255
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
tacacs server TACACS-SERVER-1
address ipv4 10.4.48.15
key 7 15210E0F162F3F0F2D2A
!
!
!
!
line con 0
line vty 0 4
access-class 55 in
exec-timeout 0 0
transport preferred none
line vty 5 15
access-class 55 in

```

```
exec-timeout 0 0
transport preferred none
!
ntp server 10.4.48.17
end
```

Outside Switch 2960S

```
version 15.0
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname OUT-2960S
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$5Ppb$vHrfB3souElPj8sw3s9i/1
!
username admin password 7 070C705F4D06485744
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
!
!
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
switch 1 provision ws-c2960s-24td-1
```

```
switch 2 provision ws-c2960s-24td-1
stack-mac persistent timer 0
!
!
ip domain-name cisco.local
ip name-server 10.4.48.10
vtp mode transparent
udld enable

!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 16-17 priority 24576
!
!
!
port-channel load-balance src-dst-ip
!
vlan internal allocation policy ascending
!
vlan 16
name ISP-A
!
vlan 17
name ISP-B
!
ip ssh version 2
!
!
!
macro name AccessEdgeQoS
auto qos voip cisco-phone
@
macro name EgressQoS
mls qos trust dscp
queue-set 1
srr-queue bandwidth share 1 30 35 5
```

```

priority-queue out
@
!
!
interface FastEthernet0
description DMZ-3750X Gig1/0/17
ip address 192.168.23.6 255.255.255.0
!
interface GigabitEthernet1/0/23
description ISP-A
switchport access vlan 16
switchport mode access
duplex full
spanning-tree portfast
!
interface GigabitEthernet1/0/24
description IE-ASA554Xa Gig0/3
switchport trunk allowed vlan 16,17
switchport mode trunk
logging event link-status
logging event trunk-status
!
interface GigabitEthernet2/0/23
description ISP-B
switchport access vlan 17
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet2/0/24
description IE-ASA5545Xb Gig0/3
switchport trunk allowed vlan 16,17
switchport mode trunk
logging event link-status
logging event trunk-status
!
interface GigabitEthernet2/0/25
!
interface GigabitEthernet2/0/26
!

```

```

interface TenGigabitEthernet2/0/1
!
interface TenGigabitEthernet2/0/2
!
interface Vlan1
no ip address
shutdown
!
ip default-gateway 192.168.23.1
no ip http server
ip http authentication aaa
ip http secure-server
!
logging esm config
access-list 55 permit 10.4.48.0 0.0.0.255
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
tacacs server TACACS-SERVER-1
address ipv4 10.4.48.15
key 7 00371605165E1F2D0A38
!
!
!
line con 0
line vty 0 4
access-class 55 in
transport preferred none
transport input ssh
line vty 5 15
access-class 55 in
transport preferred none
transport input ssh
!
ntp source FastEthernet0
ntp server 10.4.48.17
end

```

Appendix C: Changes

This appendix summarizes the changes to this guide since the previous Cisco SBA series.

- We updated the Cisco ASA firewall software to 9.0(1) with ASDM 7.0(2)
- We updated the Cisco IPS software to 7.1(6)E4
- We updated various screenshots to reflect the new software versions.
- We made minor updates to improve the usability of the guide.

Notes

Feedback

Please use the [feedback form](#) to send comments and suggestions about this guide.



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.

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

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

© 2013 Cisco Systems, Inc. All rights reserved.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)