CCNP Security Firewall 642-617 Quick Reference

Andrew Mason

Cisco Press

CCNP Security Firewall 642-617

Quick Reference

Andrew Mason

ciscopress.com

Table of Contents

About the Author

Andrew G. Mason, CCIE No. 7144, CISSP, is a security consultant and co-founder of the UK based RandomStorm Limited. Andrew has 19 years experience in the IT industry, working in Internet security for the past several years. He is involved in the design and implementation of security deployments for numerous clients based upon Cisco technology. He is also a CHECK Team Leader and leads penetration tests for many UK and international clients.

About the Technical Editor:

Max Leitch, CCIE No. 20178, is a network and security architect/engineer and an independent consultant. He holds CCNP, CCDP, CCSP, and CCIE Security certifications.

 Please see page 110 for more details.

Section 1
Cisco Firewall and ASA Technology

This Quick Reference guide provides a handy reference for students studying the Deploying Cisco ASA Firewall Features (ASAF) course and provides an easy-to-use guide for students taking the ASAF exam.

This reference is also a great refresher on the Cisco Adaptive Security Appliance (ASA) and assists the configuration and ongoing management of the range of Cisco ASA Firewalls.

This opening section of the Quick Reference guide to the Cisco ASAF exam provides an overview of firewall technologies and the features of the Cisco ASA Firewall.

Firewall Basics

A firewall is a device that connects two or more networks together and restricts the flow of information between the two or more networks according to rules configured in a firewall rule base. The firewall rule base should map to business requirements and be based on a least privilege model in which services are permitted only when they are required by the business. Firewalls have been in use for more than 20 years, but only in the past 10 years (because of the rapid growth of the Internet) has the need for firewalls increased, along with their capabilities.

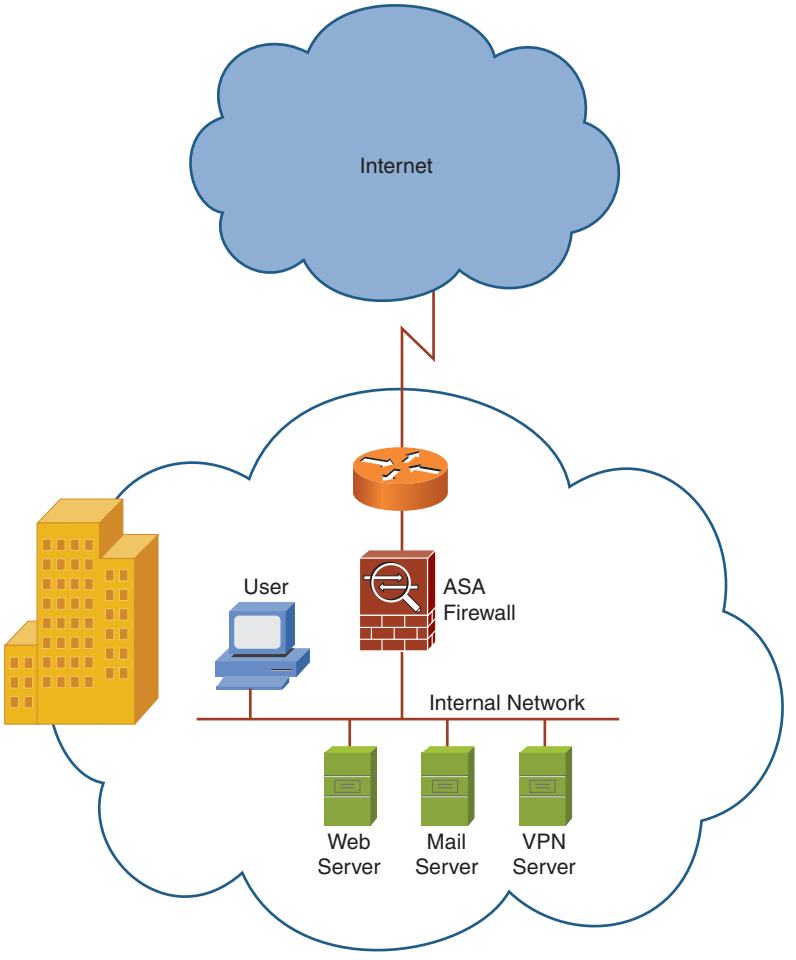
In an ideal world, a firewall would not be required. You could just allow everybody full access to all your resources, and you could trust them to access what they required. However, in the real world, firewalls have become a necessity for all organizations to limit the access to their resources to users who require access to those resources.

The Internet is a great business enabler, connecting businesses together worldwide. However, with this enabler comes a great risk. Numerous individuals and organizations specialize in hacking (breaking into other people's networks for fun or profit).

 Please see page 110 for more details.

Figure 1 shows a typical firewall deployment.

FIGURE 1
Typical Firewall Deployment



Firewalls are deployed to mitigate such risk, enabling the organization to enforce a security policy on the firewall that states what can and cannot be accessed. The firewall is only as good as the configuration deployed on it. If the configuration enables an attacker access to a resource, the firewall is not performing in its intended role as a device that protects the resources from unauthorized users.

Three types of firewalls are in use today and are based on the following technologies:

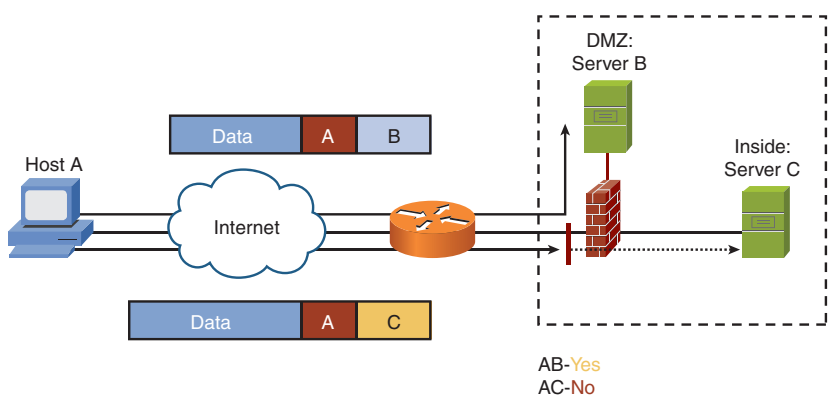
- Packet filtering
- Proxy server
- Stateful packet filtering

Packet Filtering

Packet filtering is the oldest type of firewall technology and is still put to good use today. As the name suggests, a packet filter based on an access control list (ACL) is applied to an interface to filter packets traversing the interface. The ACL dictates the security policy or firewall rule base and specifies what traffic can and cannot traverse the firewall.

Figure 2 shows a simple packet filter in place.

FIGURE 2
Packet Filtering



Most Cisco network devices perform some level of packet filtering implemented as ACLs.

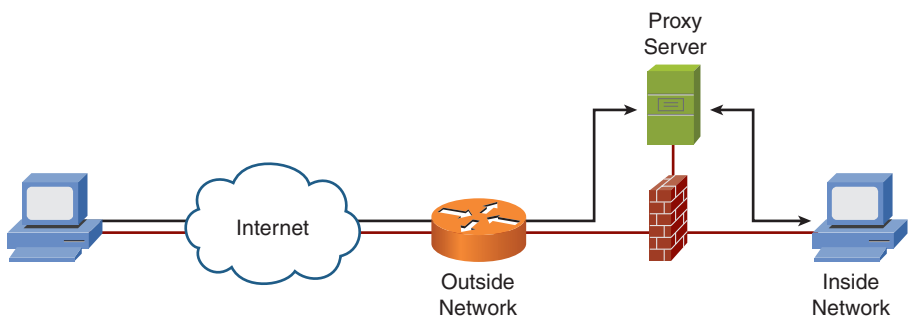
Proxy Servers

Generally, a proxy server is an application that acts as a proxy for a service. The traditional use of a proxy server has been for web traffic. In this instance, a proxy server exists on the inside of the network. Clients are configured to channel any web requests through the proxy server, which uses its own security features to restrict those who can and cannot use the service.

Because these devices operate at higher layers in the OSI model, they can be resource-intensive and might perform more slowly under stress.

Figure 3 shows the placement of a proxy server within a network.

FIGURE 3
Proxy Server



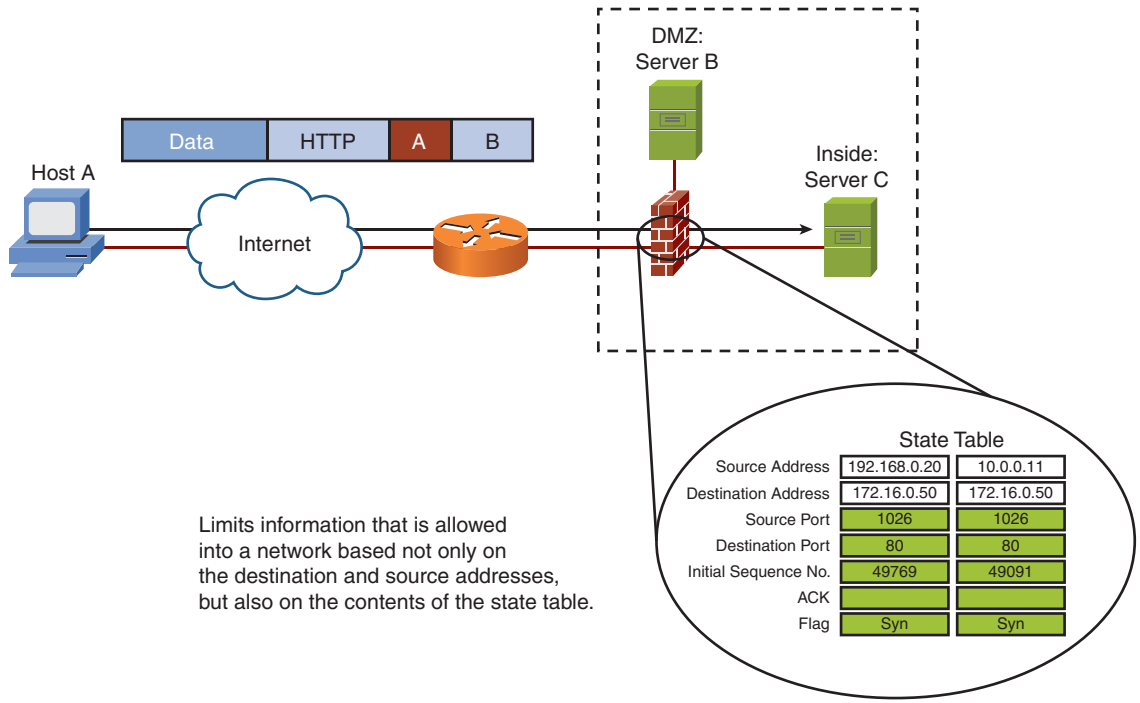
Stateful Packet Filtering

Stateful packet filtering is the method deployed by Cisco Firewall appliances. A stateful packet filter is implemented similarly to a standard packet filter, with the primary difference being that a stateful packet filter maintains complete session state. Every TCP connection or UDP flow, both inbound and outbound, is logged into the stateful session flow table.

All inbound and outbound packets are compared against the session flow table. Return data is permitted through the firewall, even though a distinct rule does not enable it based on its entry in the session table. The outbound initiation of a connection permits the return of the traffic.

Figure 4 shows stateful packet filtering.

FIGURE 4
Stateful Packet Filtering



Cisco Adaptive Security Appliance

The Cisco Adaptive Security Appliance (ASA) is a key component in the Cisco end-to-end security solution. The ASA is the market-leading Cisco security appliance and provides enterprise-class, integrated network security services.

The ASA product line offers cost-effective, easy-to-deploy solutions. The product line ranges from compact plug-and-play desktop firewalls such as the ASA 5505 for small offices to carrier-class gigabit firewalls such as the ASA 5580 for the most demanding enterprise and service-provider environments.

Cisco ASA features include the following:

- State-of-the-art stateful packet inspection firewall
- User-based authentication of inbound and outbound connections
- Integrated protocol and application inspection engines that examine packet streams at Layers 4 through 7
- Highly flexible and extensible modular security policy framework
- Robust virtual private network (VPN) services for secure site-to-site and remote-access connections
- Clientless and client-based Secure Sockets Layer (SSL) VPN
- Full-featured intrusion prevention system (IPS) services for day-zero protection against threats, including application and operating system vulnerabilities, directed attacks, worms, and other forms of malware
- Denial-of-service (DoS) prevention through mechanisms such as protocol verification to rate limiting connections and traffic flow
- Content security services, including URL filtering, antiphishing, antispam, antivirus, antispyware, and content filtering using Trend Micro technologies
- Multiple security contexts (virtual firewalls) within a single appliance
- Stateful active/active or active/standby failover capabilities that ensure resilient network protection
- Transparent deployment of security appliances into existing network environments without requiring re-addressing of the network
- Intuitive single-device management and monitoring services with the Cisco Adaptive Security Device Manager (ASDM) and enterprise-class multidevice management services through Cisco Security Manager

Cisco ASA Product Family

The Cisco ASA product family currently consists of six different models. These range in use and cost, all the way from a small office up to an enterprise or service provider network.

As you might expect, the higher the model number of the ASA, the higher the throughput, number of ports, and cost.

The product range consists of the following devices:

- Cisco ASA 5505
- Cisco ASA 5510
- Cisco ASA 5520
- Cisco ASA 5540
- Cisco ASA 5550
- Cisco ASA 5580-20
- Cisco ASA 5580-40

Figure 5 shows the Cisco ASA product family.

FIGURE 5
Cisco ASA Product Family

 Please see page 110 for more details.

Cisco ASA 5505

The ASA 5505 is available in two models: a Base model and a Security Plus model. The ASA 5505 is for small businesses, branch offices, and enterprise teleworkers.

The ASA 5505 is a small form factor appliance that is not rack mountable but more designed to sit on a desktop or within a small data cabinet:

- **Maximum throughput**: 150 Mb/s
- **Maximum connections**: 10,000 (25,000 Security Plus)
- **Maximum connections/sec**: 4000
- **Maximum VPN throughput**: 100 Mb/s
- **Maximum VPN sessions**: 10 (25 Security Plus)
- **Maximum SSL VPN sessions**: 25

Cisco ASA 5510

The ASA 5510 is available in two models: a Base model and a Security Plus model. The ASA 5510 is for deployment at the Internet edge. The ASA 5510 is a 19”-1U rack mountable appliance to be installed in data center cabinets:

- **Maximum throughput**: 300 Mb/s
- **Maximum connections**: 50,000 (130,000 Security Plus)
- **Maximum connections/sec**: 9000
- **Maximum VPN throughput**: 170 Mb/s
- **Maximum VPN sessions**: 250
- **Maximum SSL VPN sessions**: 250

 Please see page 110 for more details.

Cisco ASA 5520

The ASA 5520 is for deployment at the Internet edge. The ASA 5520 is a 19”-1U rack mountable appliance to be installed in data center cabinets.

- **Maximum throughput**: 450 Mb/s
- **Maximum connections**: 280,000
- **Maximum connections/sec**: 12,000
- **Maximum VPN throughput**: 225 Mb/s
- **Maximum VPN sessions**: 750
- **Maximum SSL VPN sessions**: 750

Cisco ASA 5540

The ASA 5540 is for deployment at the Internet edge. The ASA 5540 is a 19”-1U rack mountable appliance to be installed in data center cabinets:

- **Maximum throughput**: 650 Mb/s
- **Maximum connections**: 400,000
- **Maximum connections/sec**: 25,000
- **Maximum VPN throughput**: 325 Mb/s
- **Maximum VPN sessions**: 5000
- **Maximum SSL VPN sessions**: 2500

 Please see page 110 for more details.

Cisco ASA 5550

The ASA 5550 is for deployment at the Internet edge or within a campus network environment as an internal firewall. The ASA 5550 is a 19”-1U rack mountable appliance to be installed in data center cabinets.

- **Maximum throughput**: 1.2 Gb/s
- **Maximum connections**: 650,000
- **Maximum connections/sec**: 36,000
- **Maximum VPN throughput**: 425 Mb/s
- **Maximum VPN sessions**: 5000
- **Maximum SSL VPN sessions**: 5000

Cisco ASA 5580

The ASA 5580 is available in two models: the ASA 5580-20 and the ASA 5580-40. Both models are for the service provider or data center deployments and for use as internal firewalls for campus networks. Both ASA 5580 models are 3U 19”-rack mountable appliances to be installed in data center cabinets.

- **Maximum throughput**: 10 Gb/s (20 Gb/s 5580-40)
- **Maximum connections**: 1,000,000 (2,000,000 5580-40)
- **Maximum connections/sec**: 90,000 (150,000 5580-40)
- **Maximum VPN throughput**: 1 Gb/s
- **Maximum VPN sessions**: 10,000
- **Maximum SSL VPN sessions**: 10,000

 Please see page 110 for more details.

Service Modules

The features and functionality of the ASA can be enhanced by introducing a Security Services Card (SSC) or Security Services Module (SSM) into the ASA.

You can install SSCs into the ASA 5505, and you can install SSMs into the ASA 5510, 5520, and 5540 appliances.

Only the single SSC is available, and this is the AIP-SSC-5 that provides 75 Mbps IPS throughput for the Cisco ASA 5505.

Currently, three SSMs are available for the ASA:

- Advanced Inspection and Prevention Security Services Module (AIP SSM)
- Content Security and Control Security Services Module (CSC SSM)
- 4-Port Gigabit Ethernet SSM

Figure 6 shows a Cisco ASA SSM.

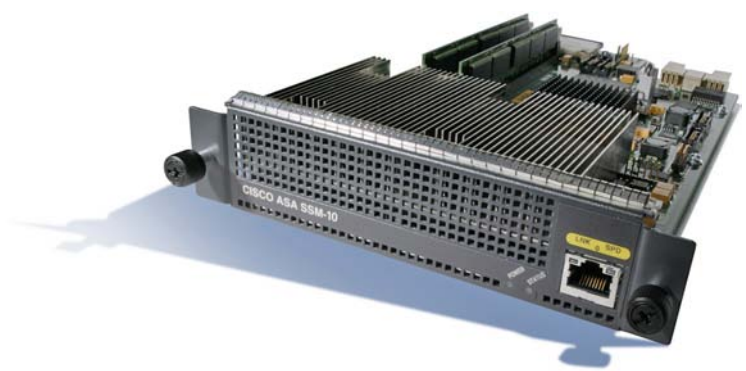


FIGURE 6
Cisco Security Services Module

 Please see page 110 for more details.

NOTE
Because the ASA has only a single SSM slot, select the appropriate SSM based on your requirements.

AIP SSM

The AIP SSM provides a full-featured IPS on a module that it used to stop malicious traffic such as viruses, worms, and directed attacks from entering your network. The AIP SSM is configured the same as the standalone Cisco IPS appliances and benefits from the same code and signature databases as the standalone IPS appliances.

Traffic is transparently redirected to the AIP module by the ASA where the AIP module performs its processing before handing the traffic back to the ASA.

The AIP SSM comes in three models:

- **AIP-SSM-10** provides 150-Mbps throughput on the ASA 5510 and 225-Mbps throughput on the ASA 5520.
- **AIP-SSM-20** provides 300-Mbps throughput on the ASA 5510, 375-Mbps throughput on the ASA 5520, and 500 Mbps throughput on the ASA 5540.
- **AIP-SSM-40** provides 450-Mbps throughput on the ASA 5520 and 650-Mbps throughput on the ASA 5540.

CSC SSM

The CSC SSM provides a content security solution within the ASA. The CSC SSM is based on software from Trend Micro that enables you to inspect traffic such as HTTP and Simple Mail Transfer Protocol (SMTP) for viruses, Trojans, and other malicious files.

The CSC SSM works in the same way as most standalone content security platforms, but one benefit is that you can totally integrate it into the ASA without incurring the cost of owning a dedicated server to perform the same role.

Traffic is transparently redirected to the SSM module by the ASA where the SSM module performs its processing before handing the traffic back to the ASA.

The CSC SSM comes in two models:

- **CSC-SSM-10** provides support for 500 users on both the ASA 5510 and 5520.
- **CSC-SSM-20** provides support for 1000 users on the ASA 5510, 5520, and 5540.

 Please see page 110 for more details.

4-Port Gigabit Ethernet SSM

The 4-port Gigabit Ethernet SSM provides an extra four ports of connectivity to the ASA. The SSM has four copper RJ-45 interfaces and four fiber small form-factor pluggable (SFP) interfaces, but only the copper or fiber interfaces can be used and not a mixture of both (which, if possible, would provide four more interface ports).

Summary

This first section provided an overview of firewall technologies and the Cisco ASA family. The next section covers the initial steps required to configure the ASA. In the next section, we examine basic Command-Line Interface (CLI) connections and how to configure the ASA through the ASDM before showing you the ways to manage the ASA device through the command-line and ASDM interfaces.

 Please see page 110 for more details.

Section 2:
Basic Connectivity and Device Management

This section starts to look at the configuration of the Cisco ASA and covers the fundamentals for providing basic connectivity and device management. This section covers basic command-line interface (CLI) configuration, but mainly focuses on configuring the ASA through the graphical Adaptive Security Device Manager (ASDM).

CLI and ASDM Connection

You can configure a Cisco ASA in two ways: through the CLI or through the ASDM.

Both the CLI and ASDM offer benefits for configuration, and people disagree as to the best method. The CLI versus GUI configuration argument has been around since the days of UNIX versus Windows. The CLI is fast, after you have mastered it, but the GUI is intuitive and easier to configure, especially with the wizard quick-configuration options now available.

ASDM is the preferred configuration method for the ASA. Various configuration wizards exist within ASDM that are not available via the CLI alone. The logging and monitoring functionality that the ASDM provides cannot be replicated within the CLI.

Command Line Interface (CLI)

The CLI is the historic way in which all Cisco devices were configured. This is a command-based interface similar to a UNIX- or DOS-based operating system.

 Please see page 110 for more details.

NOTE
Because Telnet is sent in clear text and SSH is an encrypted session, you should always use SSH to connect to any network device.

Commands are typed through a terminal connection to the ASA, and these are then written to the configuration. The CLI is powerful and fast, but learning how to use the CLI is like learning another language.

You can either connect to the CLI through the console port using a console cable or by using Telnet or Secure Shell (SSH). A Cisco console cable is provided with every ASA because this is the normal initial method to connect to the device for the initial configuration.

Using a console cable is an out-of-band connection, and using Telnet or SSH is an in-band connection.

When you first purchase an ASA, you need to configure the ASA through the CLI to configure the initial network settings that enable you to connect to the device using ASDM, which is provided through a web interface, so basic IP settings need to be initially configured.

NOTE
You can use the quick-configuration system to configure the initial parameters of the ASA to facilitate ASDM connection, but the basic con figuration commands without using the quick configuration are provided.

When you initially connect to an ASA, you are greeted with the following prompt:

```
ciscoasa>
```

This is an unprivileged mode and is represented by the **>** after the hostname.

Entering **enable** at this prompt places you into privileged EXEC mode, and you see the following prompt:

```
ciscoasa#
```

From privileged EXEC mode, you can then enter the configuration mode to enter configuration commands into the ASA. The **show** and **debug** commands to monitor and troubleshoot the ASA are also entered in privileged EXEC mode. This is similar to the EXEC modes found within IOS on a Cisco router or switch.

ASDM

ASDM is an acronym for the ASA Security Device Manager (ASDM), which it is the main graphical way to configure, manage, and monitor your ASA Firewall.

You access the ASDM through a web browser. ASDM is a Java-based application, so any modern browser that supports

 Please see page 110 for more details.

Java will suffice (for instance, Safari, Firefox, Chrome, or Internet Explorer). The connection to ASDM is over SSL, so the configuration is always encrypted between the client and the ASA through the web browser.

Because you have to connect to ASDM through a browser interface, you must configure an IP address on the inside interface to enable you to connect your browser to it. The next section covers interface configuration in more depth.

In addition to setting the IP address, you must enter some other basic configuration commands via the CLI to the ASA to configure the initial connection to the ASDM.

You now run through the necessary commands on an ASA that has a default blank configuration. The commands shown are the bare minimum to enable a connection to the ASDM and are as far as you need to take the CLI in most cases. Because this is an ASA with a blank configuration, the only way to connect is via the CLI using a serial connection.

The first step is to assign an IP address to the inside interface of the ASA. The inside interface is the interface on the inside or trusted part of your network. The outside interface is the interface on the outside or untrusted part of your network.

NOTE
For these examples, the configuration from a Cisco ASA 5505 is used, which has a built-in eight-port switch with no fixed interfaces. IP addresses on the ASA 5505 are configured to VLAN interfaces, and then the VLANs are assigned to the Ethernet interfaces. For other ASA models, the IP address is added straight to the corresponding Ethernet interface.

To enter these configuration commands, you need to be in configuration mode on the ASA. From this point forward, you should be in configuration mode; the prompt shows which configuration mode is required:

```
ciscoasa# configuration terminal
ciscoasa(config)# interface vlan 1
    ciscoasa(config-if)# ip address 192.168.1.254 255.255.255.0
```

Because this VLAN is going to be the inside network, you now need to name the VLAN interface as the inside interface:

```
Ciscoasa(config-if)# nameif inside
    INFO: Security level for "inside" set to 100 by default.
```

When the **nameif** command is entered, because the value is **inside**, the default security level of 100 is attributed to the VLAN interface. In contrast to this, the default security level of 0 would be applied to the interface if you name the interface outside.

VLAN1 is now configured as the inside interface with the IP address of 192.168.1.254/24. By default, all ports are in VLAN1, so you now need to tell the ASA 5505 which physical Ethernet port is the inside connection. In this example, you use

 Please see page 110 for more details.

Ethernet0/1 as the inside interface, so enter the following commands to bring up Ethernet0/1 because by default all ports are in an administrative shutdown mode:

```
ciscoasa(config)# interface ethernet0/1
    ciscoasa(config-if)# no shutdown
```

Running a **show interface** for Ethernet0/1 now displays the following:

```
ciscoasa# show interface ethernet0/1
Interface Ethernet0/1 "", is up, line protocol is up
  Hardware is 88E6095, BW 100 Mbps, DLY 100 usec
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        Available but not configured via nameif
        MAC address 001b.53a0.4e91, MTU not set
        IP address unassigned
        16423 packets input, 1256399 bytes, 0 no buffer
        Received 896 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 switch ingress policy drops
        6518 packets output, 5096677 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        0 rate limit drops
            0 switch egress policy drops
```

You can see that the interface is up. You can now ping the inside interface of the ASA 5505 from a workstation connected to the 192.168.1.0/24 network and ping workstations on the 192.168.1.0/24 network from the ASA 5505.

 Please see page 110 for more details.

The next step is to configure a secure password on the ASA. You can provide access to the web-based administration interface of the ASA, so ensure that it is protected and locked down with authentication.

By default there is no password set on the ASA, and anybody can connect to it via the console connection if they have physical access to the device.

Set an enable password on the ASA:

```
ciscoasa(config)# enable password securepassword
```

The preceding line creates the enable password ***securepassword***. Obviously, you would replace this with a secure, strong password in line with your corporate password policy.

At this point, the interface is up and has a valid IP address configured. However, you must complete a couple more steps to facilitate a connection to the ASDM. Running a browser to https://192.168.1.254 at this point returns with a Page Not Found error message.

The ASA has a built-in web server. This is what serves the ASDM to users requesting it through their browsers. By default, this web server is not enabled.

The internal web server in the ASA is enabled with the following command:

```
ciscoasa(config)# http server enable
```

This enables the HTTP server on the ASA, but if you tried a connection to the ASDM, you still could not connect. This failure to connect results because the ASA operates in a closed policy, unlike the HTTPS server on a router.

On the ASA, all connections to the HTTP server are denied by default, and you must enter a configuration command to specify the IP addresses that are allowed to access the ASDM. On a router, by default all IP addresses can connect to the HTTP server, and you must create an access list to restrict this access.

In this example, you want to allow the entire inside network access to the ASDM:

```
ciscoasa(config)# http 192.168.1.0 255.255.255.0 inside
```

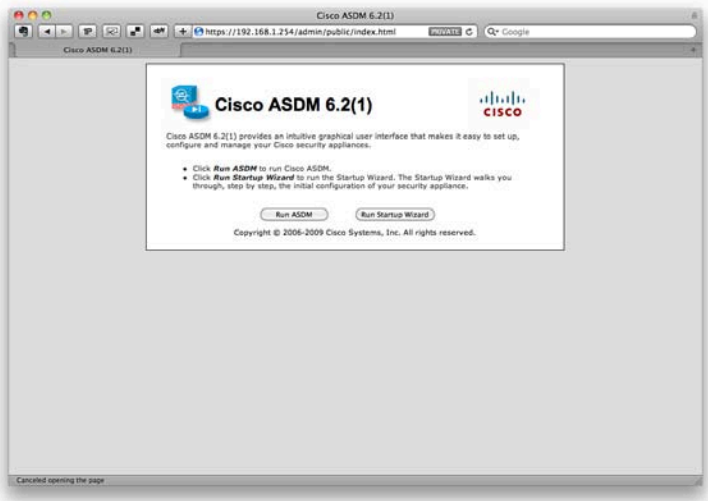
The preceding command enables all hosts on the 192.168.1.0/24 network, which is located on the inside interface, access to the

 Please see page 110 for more details.

ASDM. In the real world it is recommended that administrative access is locked down to specific management hosts, by using explicit host IP address entries.

Connecting now with a web browser to https://192.168.1.254 displays the initial ASDM connection screen, as shown in Figure 7.

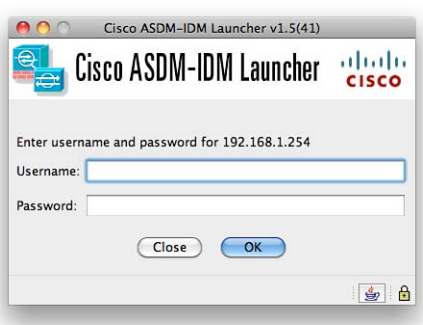
FIGURE 7
ASDM Connection Screen



You can either run the ASDM or the Startup Wizard to take you through the initial setup of the ASA. Click the **Run ASDM** button to launch ASDM.

The next window that appears asks for authentication (see Figure 8).

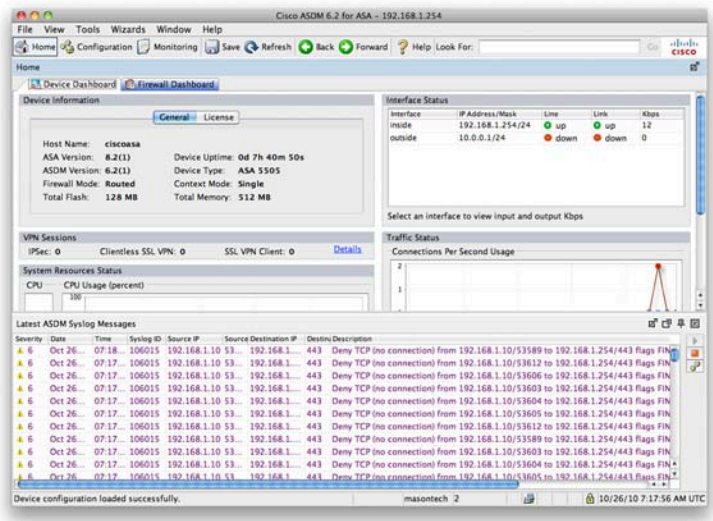
FIGURE 8
ASDM Authentication



 Please see page 110 for more details.

The authentication box requests a username and password. Because you have not configured any users on the system, you just need to enter the enable password into the Password field and leave the Username field blank.
You are now presented with a connection to the ASDM (see Figure 9).

FIGURE 9
Initial ASDM Connection



NOTE
In a real-world situation, always ensure that you use a username and password combination for authentication to the ASA. Never rely on just the enable password for authentication. This is achieved using AAA, which is covered later in this Quick Reference.

Interface Configuration Using CLI and ASDM

The ASA is a network device. Therefore, for it to function, you must configure the network interfaces for the device to operate and pass data from one interface to the other. Now look at how to configure the interface parameters via both the CLI and ASDM.

The three aspects to configuring an interface on a Cisco ASA are as follows:

- IP address and subnet mask
- Interface name
- Interface security level

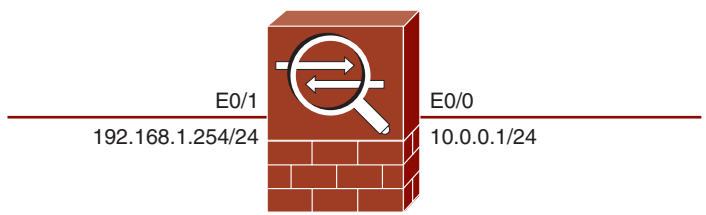
 Please see page 110 for more details.

IP Address and Subnet Mask

Each interface requires its own IP address that exists in a different subnet. The ASA can operate in two modes: routed and transparent. For these examples, use routed mode (the default). Transparent mode is covered in Section 4, "ASA Network Integration," of this Quick Reference guide.

You have already applied an IP address of 192.168.1.254/24 to the inside interface of the ASA. Now configure the IP address of 10.0.0.1/24 to the outside interface. This setup follows the simple network diagram shown in Figure 10.

FIGURE 10
Simple ASA Network



To assign an IP address to an interface, use the **ip address** command from interface configuration mode. The following example sets the IP address of 10.0.0.1/24 to Ethernet0/0:

```
ciscoasa(config)# interface ethernet0/0
    ciscoasa(config-if)# ip address 10.0.0.1 255.255.255.0
```

In this example, you use an ASA 5505, and you already assigned an IP address of 192.168.1.254/24 to the VLAN1 interface. The configuration command for this is as follows:

```
ciscoasa(config)# interface vlan1
    ciscoasa(config-if)# ip address 192.168.1.254 255.255.255.0
```

Interface Name

All interfaces on an ASA must be given a name. These names are used in other configuration items, such as Network Address Translation (NAT) and access control lists (ACL). Some common and also default names when configuring the ASA include outside, inside, and DMZ. It is worthwhile to provide a meaningful name because this can help with understanding your configuration.

 Please see page 110 for more details.

To give Ethernet0/1 the name of inside, issue the following command:

```
ciscoasa(config)# interface ethernet0/1
     ciscoasa(config-if)# nameif inside
```

In this example, use an ASA 5505 and assign the name of inside to the VLAN1 interface. The configuration command for this is as follows:

```
ciscoasa(config)# interface vlan1
     ciscoasa(config-if)# nameif inside
```

Interface Security Level

The ASA in its default state uses interface security levels to determine traffic flow and to ascertain what action the appliance should take on traffic traversing it. Every interface must have a security level. This originated from a PIX technology called the Adaptive Security Algorithm (confusingly, also known as ASA).

Following are two important factors:

- Traffic from a higher-security interface to a lower-security interface is enabled by default. This is classed as outbound traffic. Configuration is required to enable the traffic, but it will flow without the use of ACLs.
- Traffic from a lower-security interface to a higher-security interface is disallowed by default. This is classed as inbound traffic. The use of ACLs is required to enable inbound traffic.

Some default security levels are assigned to interfaces. By default, the outside named interface always has a security level of 0, and the inside named interface has a security level of 100.

The minimum security level is 0, and the maximum security level is 100. Therefore, these two interfaces are placed at either end of the scale and thus enable additional interfaces, such as the DMZ, to be placed between these values to further enhance the security design of the network.

 Please see page 110 for more details.

It is common for a DMZ interface to be assigned a security level of 50.

To give Ethernet0/1 the security level of 100, issue the following command:

```
ciscoasa(config)# interface ethernet0/1
    ciscoasa(config-if)# security-level 100
```

In this example, use an ASA 5505, and assign the name of inside to the VLAN1 interface. This configuration means that this interface will have a security level of 100. The configuration command for this is as follows:

```
ciscoasa(config)# interface vlan1
    ciscoasa(config-if)# security-level 100
```

ASDM Interface Configuration

You can configure an interface via ASDM from a single configuration screen.

You must select **Configuration** from the toolbar, and then **Device Setup**. You can then add, edit, or delete interfaces from the configuration.

Because you have already configured the inside interface in your example as VLAN1, now enhance this by configuring only VLAN1 on the Ethernet0/1 physical port.

Highlight the inside interface, and then click **Edit**. Figure 11 shows the Edit Interface screen. As you can see from Figure 11, the IP address, interface name, and security level can all be entered into the ASA configuration from this single screen. In this example, you can see that Ethernet0/1 has been selected and has an IP address of 192.168.1.254/24, with an interface name of inside and a security level of 100.

No firewall is complete with a single interface, so go ahead and configure the outside interface of the ASA.

 Please see page 110 for more details.

FIGURE 11
ASDM Interface Configuration

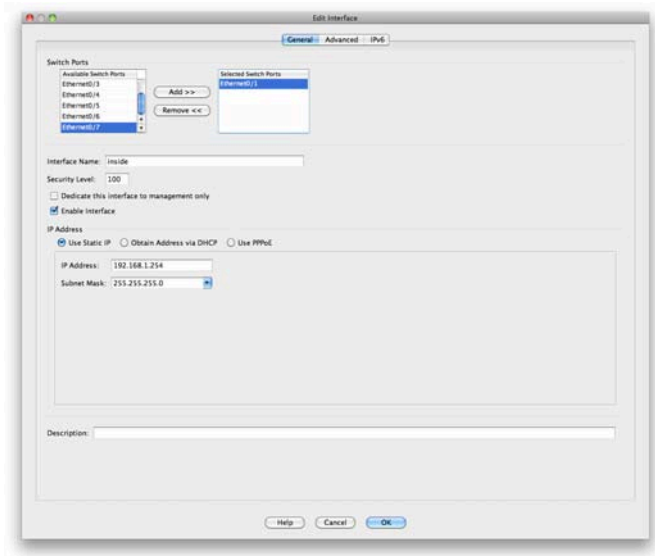
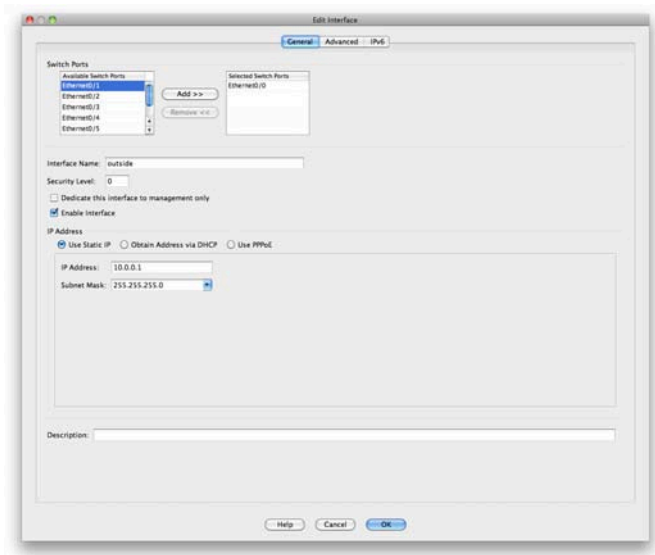


Figure 12 shows the configuration screen on the ASA for the outside interface.

FIGURE 12
ASDM Outside Interface Configuration

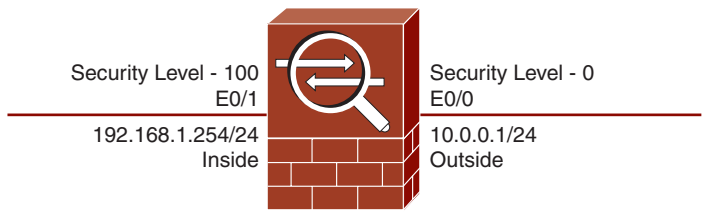


 Please see page 110 for more details.

You can see in Figure 12 that Ethernet0/0 is assigned an IP address of 10.0.0.1/24. This interface is named outside and given a default security level of 0.

You now have the network as shown in Figure 13.

FIGURE 13
Simple Network with the ASA



Now the interfaces are configured, so move on and look at the ways to connect to the ASA.

Telnet and SSH Access to the ASA

You have already connected to the ASA through the console cable and through the ASDM. You can also configure Telnet and SSH access to the ASA to perform a command-line configuration.

Telnet Configuration

Telnet is a protocol used for connecting to line-based applications. Telnet traffic is sent in clear text, so you never want to use Telnet outside of a private network. SSH is always a better option, and Telnet should be used only when SSH is unavailable.

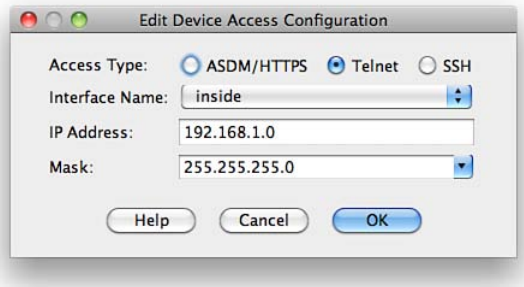
You can enable Telnet to the ASA through any interface. The only caveat is that Telnet to the outside interface must be protected by IPsec, so direct Telnet access to an outside interface is not enabled.

To configure Telnet, navigate **to Device Management > Management Access > ASDM/HTTPS/Telnet/SSH**.

From this screen, add the Telnet configuration ensuring that Telnet is selected as the Access Type, as shown in Figure 14.

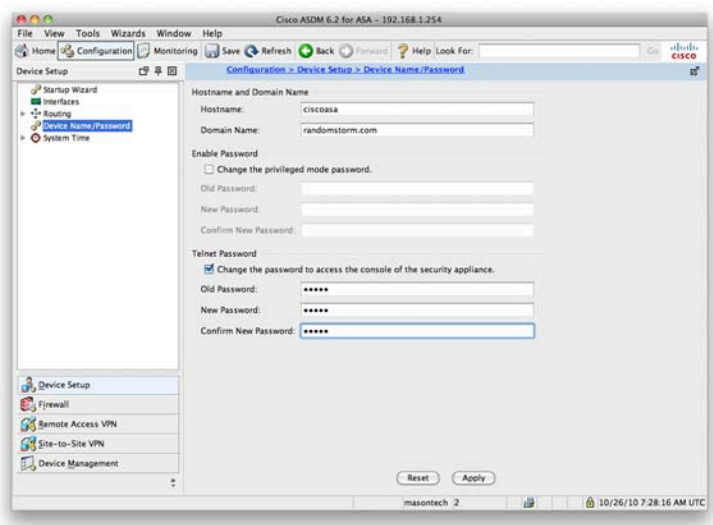
 Please see page 110 for more details.

FIGURE 14
Add Telnet Configuration



In Figure 14 you have enabled Telnet access on the inside interface for the network 192.168.1.0/24.
You now have to enter a Telnet password into the ASA. Navigate to **Device Setup > Device Name/Password**. Click the check box to change the Telnet password. By default, the old password is set to cisco. Enter a new secure password, and then apply it. Figure 15 shows the Device Name/Password screen.

FIGURE 15
Device Name/ Password



Telnet is now configured on the ASA, and users on the 192.168.1.0/24 network can telnet to the ASA.

 Please see page 110 for more details.

SSH Configuration

SSH connection is the preferred method over Telnet. Because SSH provides strong authentication and encryption, SSH provides secure remote access to the CLI of the ASA.

Steps required to enable SSH follows:

Step 1: Configure the hostname.

Step 2: Configure the Domain Name.

Step 3: Generate the RSA keys.

Step 4: Configure the local authentication.

Step 5: Configure SSH on the specific interface.

SSH configuration is similar to Telnet configuration. To configure SSH, navigate to **Device Management > Management Access > ASDM/HTTPS/Telnet/SSH**.

As you did with Telnet, specify an interface, IP address, and subnet mask for the network that you want to grant SSH access to. You can use SSH on the outside interface without requiring IPsec because SSH supports strong authentication and encryption. Be sure to select SSH as the Access Type when entering the details.

You require the Telnet password to be set so that you can use SSH to connect into an ASA. From the ASA client, you need to enter a command similar to the following:

```
userpc$ssh pix@192.168.1.254
```

You are then prompted for the password; enter the password you configured as the Telnet password. When you use SSH to connect into an ASA, the username you use is **pix**.

Software Image Configuration

The ASA relies on two main software images. The first is the ASA software image that runs the core operating system of the ASA. The second is the ASDM image. The ASA works as a firewall without the ASDM image, but you cannot access ASDM and can configure only the ASA with the CLI.

When you initially purchase an ASA, it comes with both an ASA software image and an ASDM software image already preinstalled on the ASA flash memory.

Command-Line Software Image Configuration

From the CLI, the command **show flash displays** which software images are located in the flash memory of the ASA:

```
ciscoasa# show flash
--#--  --length--  -----date/time------  path
   87  4181246     Jun 08 2010 20:56:48  securedesktop-asa-3.2.1.103-k9.pkg
    88  398305      Jun 08 2010 20:57:08  sslclient-win-1.1.0.154.pkg
   10  4096        Jun 08 2010 21:01:12  crypto_archive
    91  16275456    Sep 28 2010 05:53:22  asa821-k8.bin
    92  11348300    Sep 28 2010 05:55:02  asdm-621.bin
     3  4096        Sep 28 2010 05:56:26  log
    11  4096        Oct 07 2010 08:38:48  coredumpinfo
    12  43          Oct 10 2010 11:28:26  coredumpinfo/coredump.cfg

127111168 bytes total (79499264 bytes free)
    ciscoasa#
```

From the preceding output, you can see eight files in the ASA flash. The ones you are interested in are asa821-k8.bin and asdm-621.bin.

 Please see page 110 for more details.

The asa821-k8.bin file is the software image for the ASA (in this case, version 8.21). The asdm-621.bin file is the ASDM software image (in this case, version 6.21). The other files include the Secure Desktop, the SSL client, and the log file generated by the ASA.

To add a file to flash from the CLI, use the **copy** command. For example, to copy a file from TFTP to flash, use the following:

```
ciscoasa# copy tftp flash
```

You are then prompted for the address of the remote TFTP server and the remote filename. In addition to TFTP, the following options are now available with the **copy** command:

```
ciscoasa# copy ?
  /noconfirm      Do not prompt for confirmation
  /pcap            Raw packet capture dump
  capture:         Copyout capture buffer
  disk0:           Copy from disk0: file system
  flash:          Copy from flash: file system
  ftp:             Copy from ftp: file system
  http:            Copy from http: file system
  https:           Copy from https: file system
  running-config  Copy from current system configuration
  smb:             Copy from smb: file system
  startup-config  Copy from startup configuration
  system:          Copy from system: file system
      tftp:            Copy from tftp: file system
```

As long as there is a single ASA software image in the flash, the ASA will always boot from this. If there are two or more ASA images in the flash, you need to use the **boot system** command from global configuration mode to tell the ASA which boot image to use.

For example, to boot from the image asa821-k8.bin stored in flash, the command would be as follows:

 Please see page 110 for more details.

```
ciscoasa(config)# boot system flash:/asa821-k8.bin
```

If you have multiple ASDM images in flash, you need to use the ASDM image command from global configuration mode to tell the ASA which ASDM image to use. For example, to use the image asdm-621.bin stored in flash as the ASDM image the configuration command follows:

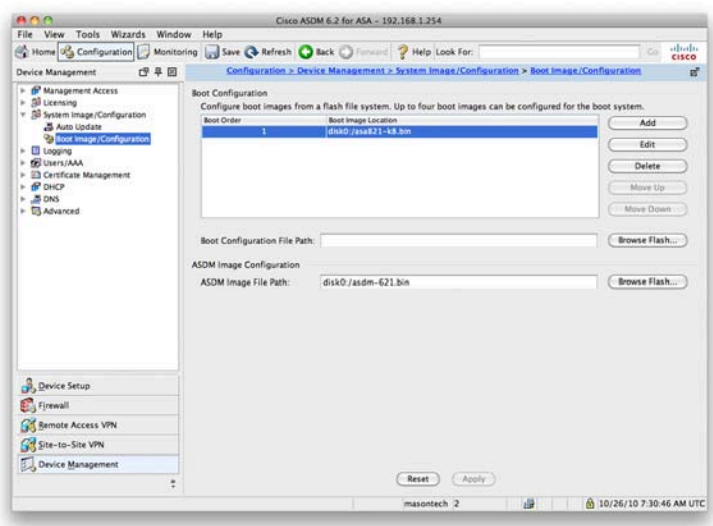
```
ciscoasa(config)# asdm image flash:/asdm-621.bin
```

ASDM Software Image Configuration

From the ASDM, navigate to the Device Management > System Image/Configuration > Boot Image/Configuration screen.

From this screen, you can add files to flash, remove files from flash, set the ASA boot image, and set the ASDM image (see Figure 16).

FIGURE 16
Boot Image/
Configuration



 Please see page 110 for more details.

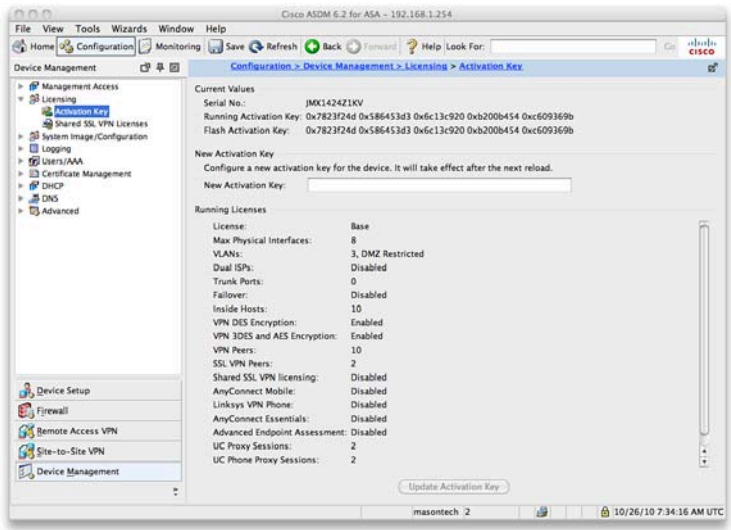
Licensing the ASA

The ASA is licensed with the use of activation keys. The activation key is tied to the serial number of the ASA, which is hard-coded into the operating code of the ASA.

To enable a feature, you need to purchase the required license. You then redeem this with Cisco after providing your serial number, at which time you will be provided an activation key. Because it is tied to the serial number, this activation key works only on the ASA for which it was requested.

Navigate to **Device Management > Licensing > Activation Key**, and enter the new activation key (see Figure 17).

FIGURE 17
Activation Key



 Please see page 110 for more details.

The current license and features can be seen from the Home screen and the Device Dashboard in ASDM as well as from this screen where the exact license details and what is enabled on the ASA you are connected to are shown.

From the CLI, the **show version** command also provides information about the current licensing as shown in bold:

```
ciscoasa# show version

Cisco Adaptive Security Appliance Software Version 8.2(1)
Device Manager Version 6.2(1)

System image file is “disk0:/asa821-k8.bin”

Hardware:   ASA5505, 512 MB RAM, CPU Geode 500 MHz
Internal ATA Compact Flash, 128MB
BIOS Flash Firmware Hub @ 0xffe00000, 1024KB

Encryption hardware device : Cisco ASA-5505 on-board accelerator (revision 0x0)
                             Boot microcode   : CN1000-MC-BOOT-2.00
                             SSL/IKE microcode: CNLite-MC-SSLm-PLUS-2.03
                             IPSec microcode  : CNlite-MC-IPSECm-MAIN-2.04
 0: Int: Internal-Data0/0    : address is c84c.757d.41a1, irq 11
 1: Ext: Ethernet0/0         : address is c84c.757d.4199, irq 255
 2: Ext: Ethernet0/1         : address is c84c.757d.419a, irq 255
 3: Ext: Ethernet0/2         : address is c84c.757d.419b, irq 255
 4: Ext: Ethernet0/3         : address is c84c.757d.419c, irq 255
 5: Ext: Ethernet0/4         : address is c84c.757d.419d, irq 255
 6: Ext: Ethernet0/5         : address is c84c.757d.419e, irq 255
 7: Ext: Ethernet0/6         : address is c84c.757d.419f, irq 255
 8: Ext: Ethernet0/7         : address is c84c.757d.41a0, irq 255
 9: Int: Internal-Data0/1    : address is 0000.0003.0002, irq 255
10: Int: Not used            : irq 255
11: Int: Not used            : irq 255
```

 Please see page 110 for more details.

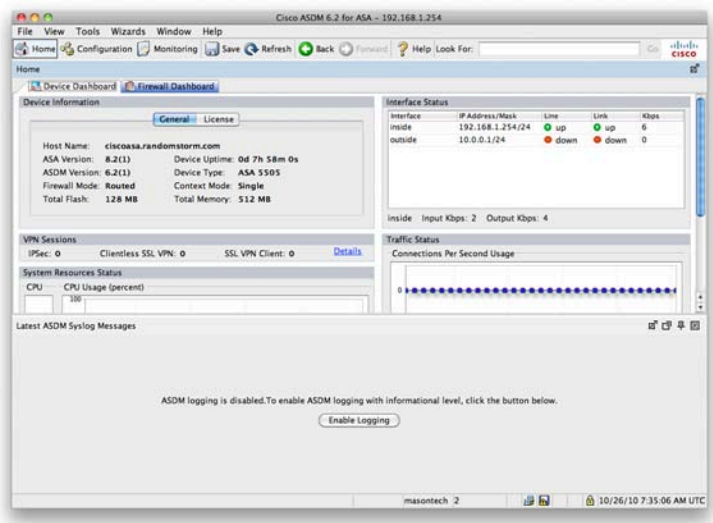
```
Licensed features for this platform:
Maximum Physical Interfaces  : 8
VLANs                        : 3, DMZ Restricted
Inside Hosts                 : 10
Failover                     : Disabled
VPN-DES                      : Enabled
VPN-3DES-AES                 : Enabled
SSL VPN Peers                : 2
Total VPN Peers              : 10
Dual ISPs                    : Disabled
VLAN Trunk Ports             : 0
Shared License               : Disabled
AnyConnect for Mobile        : Disabled
AnyConnect for Linksys phone : Disabled
AnyConnect Essentials        : Disabled
Advanced Endpoint Assessment : Disabled
UC Phone Proxy Sessions      : 2
Total UC Proxy Sessions      : 2
Botnet Traffic Filter        : Disabled

This platform has a Base license.

Serial Number: JMX1424Z1KV
Running Activation Key: 0x7823f24d 0x586453d3 0x6c13c920 0xb200b454 0xc609369b
Configuration register is 0x1
Configuration last modified by masontech at 11:28:16.419 UTC Sun Oct 10 2010
    ciscoasa#
```

 Please see page 110 for more details.

Configuring Logging on the ASA

Logging is disabled by default on the ASA. When you first connect to the ASDM, the first screen you see is the Home screen and the Device Dashboard (see Figure 18).

FIGURE 18
Device Dashboard

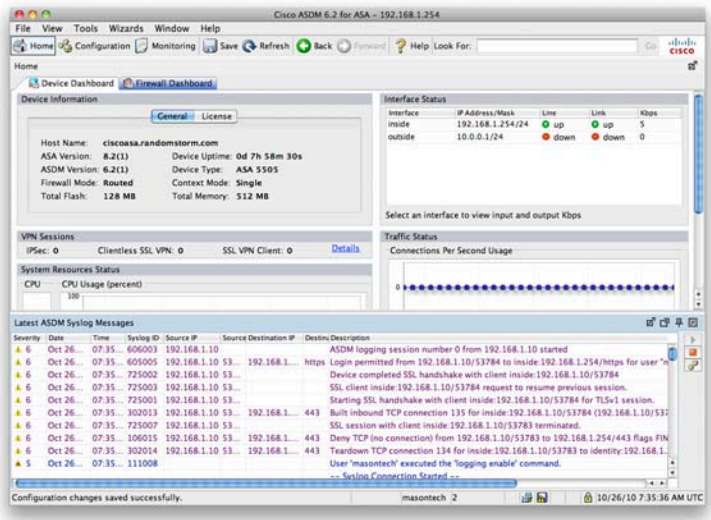


You can see from Figure 18 that ASDM logging is disabled. There is a button in the bottom half of the screen that can enable logging. Clicking this button enables logging on the ASA.
Figure 19 shows logging information on the Device Dashboard.

When logging is enabled, you can see the real-time log events in the Device Dashboard. You can also monitor logging events from the Monitoring toolbar.

 Please see page 110 for more details.

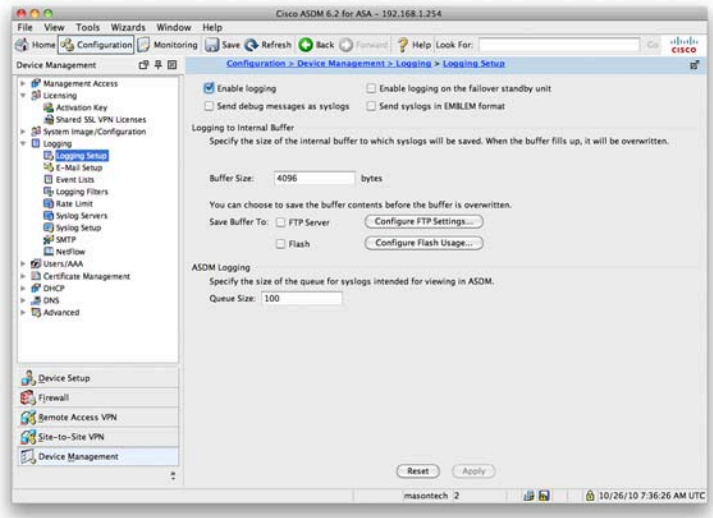
FIGURE 19
Device Dashboard: Logging Enabled



From the Configuration toolbar, navigating to **Device Management > Logging** provides you with more in-depth configuration options for configuring items such as external logging servers, log filters, and external email addresses. Figure 20 shows the Logging Setup screen.

 Please see page 110 for more details.

FIGURE 20
Logging Setup



Summary

This section covered the initial configuration of the Cisco ASA and started by looking at using the CLI and ASDM for configuration and then moved on to how to configure IP addresses on the interfaces and names and security levels.

Then the management and monitoring of the ASA was covered. Configuring the ASA for Telnet and SSH connections and how to manage the software images on the ASA through the CLI and ASDM were explored. Licensing of the ASA and where to go to get logging statistics from the ASA about the traffic traversing it was discussed.

The next section starts to delve more into the configuration of the ASA for access control starting with Network Address Translation (NAT) moving onto access lists and advanced features such as the Modular Policy Framework (MPF).

 Please see page 110 for more details.

Section 3
ASA Access Control

Now that you have connectivity to the ASA and have configured basic networking settings on the ASA, you can start to look at making the ASA operate as a true firewall.

This section covers the services offered by the ASA such as Network Address Translation (NAT) and Access Lists that make up the main foundation of protection offered by the Cisco ASA.

Network Address Translation

Network Address Translation (NAT) is a key concept and technology used by the ASA. The main purpose of NAT is to translate one IP address into another. It is commonly used to translate private IP addresses into publicly routable IP addresses for use over the Internet.

One of the main uses of NAT is at the perimeter of the corporate network. Good network design dictates that corporate networks use a private IP addressing scheme as defined by RFC 1918. This includes the following addresses for use within corporate networks:

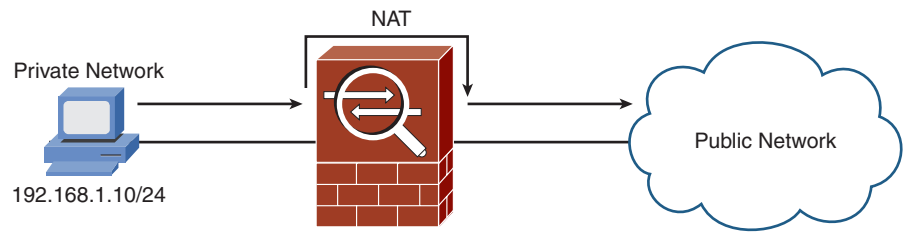
- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

The preceding networks are not publically routable on the Internet. Therefore to communicate on the public Internet you need to translate these private addresses into a public address. A public address is usually assigned by an Internet service provider and is an address outside of the RFC 1918 private range. For example, 194.73.134.1 is considered a public IP address.

 Please see page 110 for more details.

Figure 21 shows how NAT would be used in the simple network you configured on the ASA.

FIGURE 21
Simple NAT with the ASA



NAT, in the true sense, translates one address to another address. There is also a subfunction of NAT called Port Address Translation (PAT), which is where multiple internal addresses are translated into a single external address. Different source ports are used on the external address to differentiate between the internal addresses, and this information is held by the device performing the translation so that it can work out where to send the return packets. PAT is also commonly referred to as NAT-Overload.

On the ASA, NAT is required when traffic is flowing from a lower-security interface to a higher-security interface. For example, the outside interface has a security level of 0, and the inside interface has a security level of 100. Therefore, NAT is required for hosts on the outside to communicate with hosts on the inside.

NAT is not required by default for traffic flowing from a higher-security interface to a lower-security interface. This has been the case since Cisco released PIX and ASA 7.0. You can enable this setting by issuing the **nat-control** command, which then forces the use of NAT on all interfaces in all directions.

Simple NAT Configuration

To configure NAT on the ASDM, choose Configuration from the toolbar and then Firewall. NAT rules are created on the ASA and perform the translations depending on the configuration. By default, no NAT rules are configured on the ASA.

You can add three main types of NAT rules: static, dynamic, and exempt.

 Please see page 110 for more details.

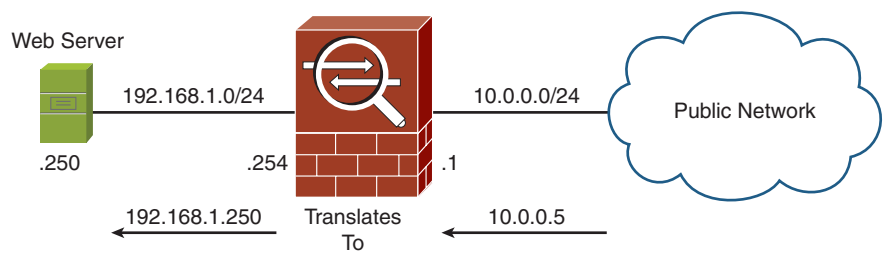
Start these examples by adding a static NAT rule.

Adding a Static NAT Rule with ASDM

Static NAT is where you can perform a one-to-one NAT translation; a single internal IP address is translated to a single external IP address. This is normally used for inbound access where external users are accessing resources such as a corporate web or email server.

Figure 22 shows the inclusion of a web server in your simple network topology.

FIGURE 22
Web Server



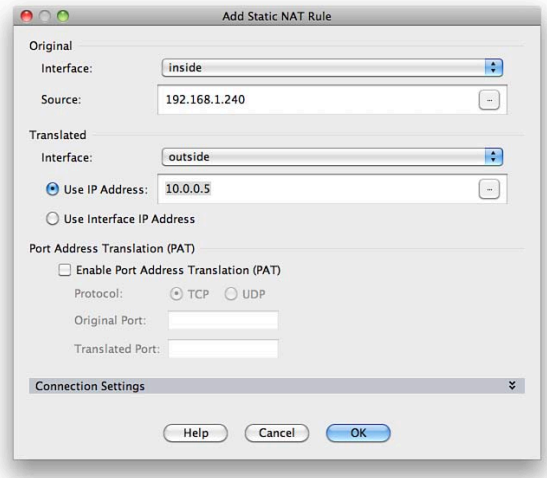
The web server has an internal IP address of 192.168.1.250/24. Hosts from the outside cannot access this server on this address because it is not routable via the outside interface (because a NAT translation is required).

What we need to configure is a static NAT entry from 192.168.1.250 that translates to 10.0.0.5. Doing so then enables external users to access the web server on 10.0.0.5.

Figure 23 shows a static NAT translation and the settings.

 Please see page 110 for more details.

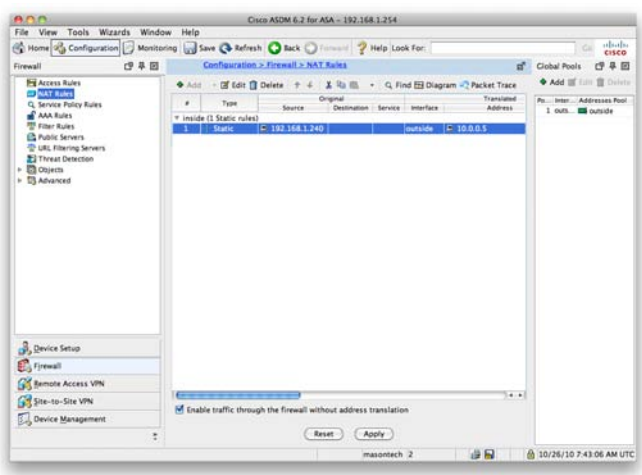
FIGURE 23
Static NAT Configuration



You can see in Figure 23 the entered original and translated addresses into the ASDM. This setting can translate 192.168.1.250 to 10.0.0.5 on the outside interface. When applying this setting, you then go back to the NAT Rules configuration screen shown in Figure 24. This screen lists all the configured NAT rules on the ASA, which in this case is only the single static NAT rule.

Now that you have configured a static NAT rule through the ASDM, the next rule to look at is a dynamic NAT rule.

FIGURE 24
NAT Rules Screen



 Please see page 110 for more details.

Adding a Dynamic NAT Rule with ASDM

Static NAT translations provide a one-to-one translation of IP addresses. A dynamic NAT rule creates a one-to-many translation of IP addresses.

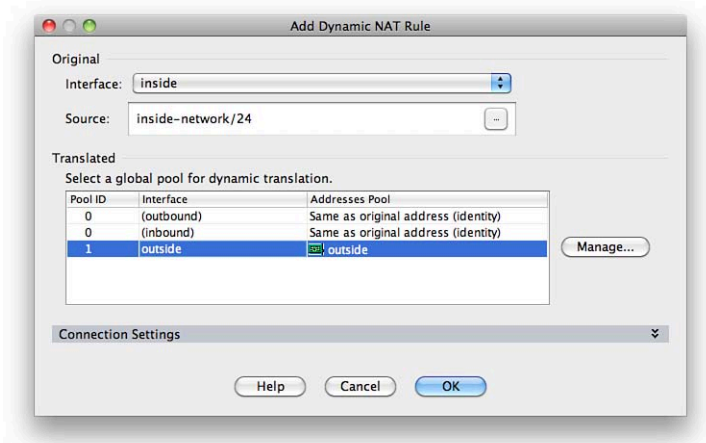
The most common use of dynamic NAT is when the ASA is placed at the network perimeter between the corporate network and the Internet. Users on the corporate network want Internet access, so they require a NAT translation to translate their private IP address to a publicly routable IP address. If there are 50 internal users, you would require 50 public addresses for the translation if you use a static NAT translation.

Dynamic NAT uses a single public IP address and enables all the internal users access to the Internet. They all use the same public IP address and are tracked by the ASA by using different source ports for each internal client.

When you add a dynamic NAT rule, you need to link it to an address pool. You can create these address pools via **Objects > Global Pool**, or you can create them while adding the dynamic NAT rule.

Figure 25 shows a dynamic NAT rule that applies to 192.168.1.0/24 and uses the address of the outside interface for the translation.

FIGURE 25
Adding a Dynamic NAT Rule

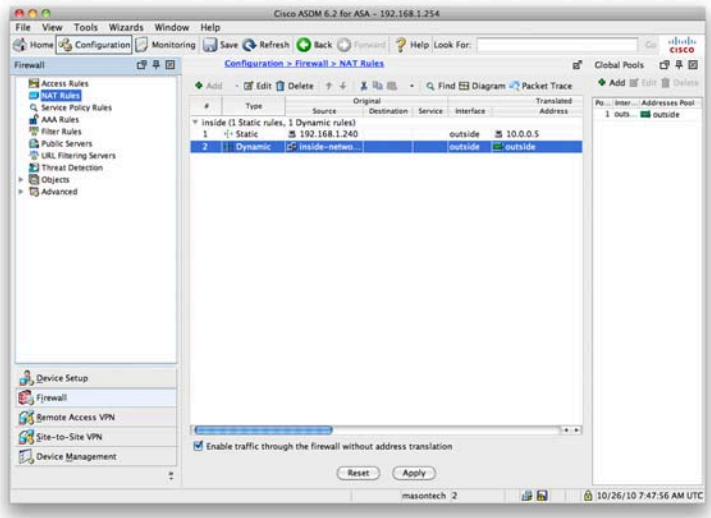


When you apply this rule, you go back to the NAT Rules screen. On this screen, as shown in Figure 26, you see a configured static NAT rule and a dynamic NAT rule.

The last type of NAT rule to look at is a NAT exempt rule.

 Please see page 110 for more details.

FIGURE 26
NAT Rules Screen



Adding a NAT Exempt Rule with ASDM

You have just configured static and dynamic NAT on the ASA via ASDM. Now look at the third option available when adding a NAT rule: a NAT exempt rule.

NAT exemption exempts addresses from NAT translation. When NAT is configured on an interface, you sometimes might need a specific host to bypass NAT and be exempt from the NAT rules. A common use of this is when configuring VPNs and you want the local private network to communicate with the remote private network without being translated.

Access Lists

You just looked at configuring NAT on the ASA. Now that you have configured NAT, the next element to look at is ACLs, which are the restrictive lists that define the firewall. These are also called a firewall rule set or rule base. The ACL is one of the most important aspects of the firewall because it permits and denies traffic through the firewall. The incorrect configuration of an ACL can result in a security hole that a potential attacker may use to exploit an internal system. Without an ACL, a firewall is not much more than a standard router.

 Please see page 110 for more details.

Configuring ACLs with ASDM

In the example, you have shown a web server on the inside of the network. This web server has a static NAT translation. Now provide an ACL that enables inbound traffic matching the web server address to access the web server.

To configure ACLs, from the toolbar select **Configuration** and then **Firewall > Access Rules**.

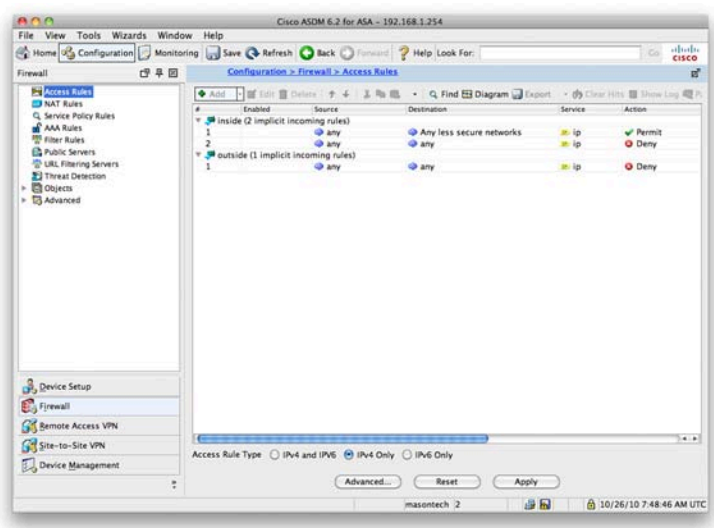
You see that by default some rules are already applied to the ASA, which are the implicit rules configured by default on the ASA device. These rules cannot be removed; they are the catchall rules matched if no other rule is matched first.

Figure 27 shows these implicit rules. Looking at Figure 27, you can see three implicit access rules. Two are applied to the inside interface and one to the outside interface.

The implicit access rules applied to the inside interface are as follows:

- Permit traffic from anywhere destined to a lower-security interface.
- Deny any traffic from anywhere to anywhere.

FIGURE 27
Implicit Access Rules



 Please see page 110 for more details.

This rule implements the ASA mentioned earlier. Any traffic from the inside interface is permitted only to lower-security interfaces. All other traffic is denied.

The implicit access rule applied to the outside interface is as follows:

- Deny any traffic from anywhere to anywhere.

Because the outside interface has the lowest available security level (0), all traffic is by default denied unless a more specific access rule permits it. This default ensures that nothing enters the firewall from the outside without previous configuration.

Clicking Add brings up the Add an Access Rule screen. You need to add a rule on the outside interface to enable access to the internal web server on TCP port 80.

Figure 28 shows the completed screen to create this access rule.

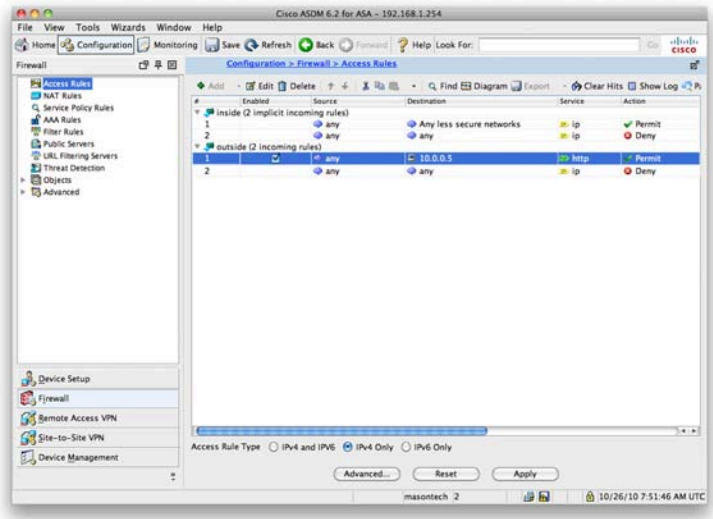
FIGURE 28
Add an Access Rule

You can see from Figure 28 that you created a rule that permits TCP port 80/HTTP traffic from anywhere to access the outside interface and the address 10.0.0.5. This is the address you used for the static NAT translation for the web server.

Applying this access rule takes you back to the Access Rules screen of the ASDM, as shown in Figure 29. You can now see the new rule that has been configured on the outside interface and has been placed above the implicit rule that denies all other traffic. Traffic can now access the website from anywhere on the Internet.

 Please see page 110 for more details.

FIGURE 29
Access Rules Screen

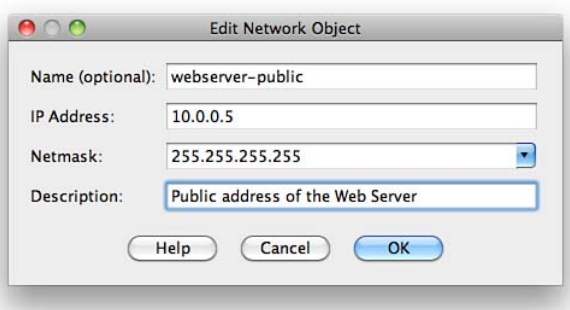


Using Object Groups Within ACLs

You now want to extend this further and permit HTTPS into the web server. You also want to use the name **webserver-public** rather than the public IP address of the web server. You can achieve both of these goals by configuring objects on the ASA.

Start by defining the web server as an object within the ASA. Navigate to **Firewall > Objects > Network Objects/Groups**. Add an entry using the public IP address of the web server and the name of **webserver-public**. You can see this completed in Figure 30.

FIGURE 30
Configure an IP Name



 Please see page 110 for more details.

You have now configured a more meaningful name for the public IP address of the web server. Next configure an access rule to also enable HTTPS access to the web server. You could just add another access rule that permits HTTPS from anywhere to the web server, as you did with the initial access rule that permitted HTTP. However, you can achieve this is by creating a service group. Navigate to **Firewall > Objects > Service Groups**, and then click **Add** to add a new service group.

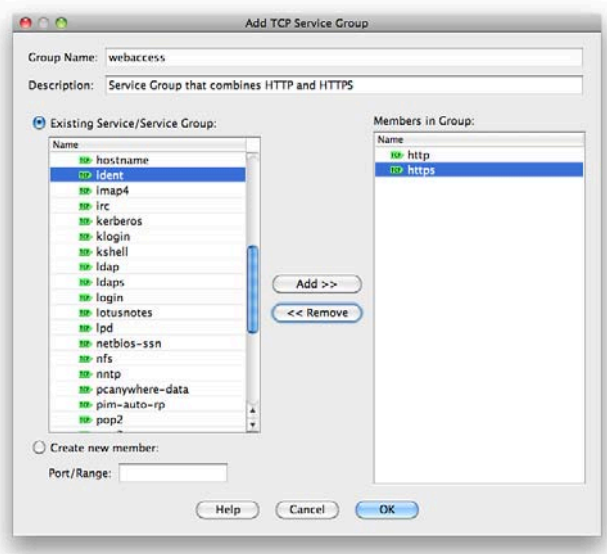
Because both HTTP and HTTPS are TCP protocols, you need to select **TCP Service Group**. Call the group **webaccess** and add both HTTP and HTTPS to the group.

Figure 31 shows that you created a single TCP service group called **webaccess** that now contains these two protocols.

The next step is to go back to the Access Rules configuration screen and change the existing access rule to use the new group.

When you navigate to **Firewall > Access Rules**, the destination field for the access rule that you created has now changed from 10.0.0.5 to **webserver-public**. This is because you added the IP name object for the web server. From now on, the ASA will know 10.0.0.5 as **webserver-public**, making it easier to read the rule base and understand it.

FIGURE 31
Edit TCP Service Group



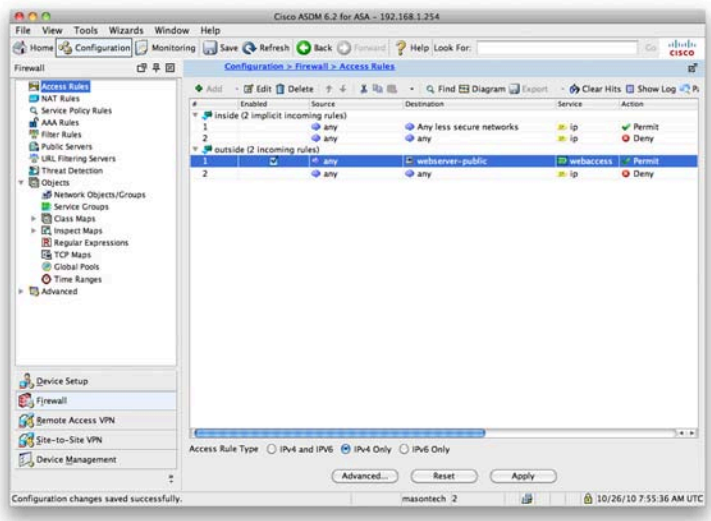
 Please see page 110 for more details.

Highlight the rule you created earlier, and click **Edit**. Select the service by clicking the ellipsis (**…**) button next to the service. Now add the TCP service group that you have just created. The service group should be at the top of the list. Select it and click **OK** to return to the main Access Rules screen, as shown in Figure 32.

Figure 32 shows that the destination name is now **webserver-public** and the service is now **webaccess** and not HTTP.

You just created a single rule that enables both HTTP and HTTPS access inbound on the outside interface to the public address of the web server.

FIGURE 32
Access Rules Screen



Modular Policy Framework

The Modular Policy Framework (MPF) is an advanced feature of the ASA that provides the security administrator with greater granularity and more flexibility when configuring network policies. The security administrator can do the following:

- Define flows of traffic.
- Associate security policies to traffic flows.
- Enable a set of security policies on an interface or globally.

Modular policies consist of the following components:

- Class maps
- Policy maps
- Service policies

Class Maps

A class map is a configuration element used to match something. A class map is similar in operation to an access control list (ACL), but with class maps you can match other items that ACLs cannot match.

Class maps can define a class of traffic by matching via the follow command keywords:

- **access list**: An entry in an ACL.
- **any:** Any packet.
- **default inspection traffic**: The default TCP and UDP ports used by all applications that the security appliance can inspect. You can specify an ACL-based class along with the default inspection traffic class to narrow the matched traffic.
- **dscp**: A differentiated services code point (DSCP) value in the IP header defined by the Internet Engineering Task Force (IETF).
- **flow**: All traffic going to a unique IP destination address.

 Please see page 110 for more details.

- **port**: Traffic using the TCP or UDP destination port or a contiguous range of ports.
- **precedence**: The precedence value represented by the Type of Service (ToS) byte in the IP header.
- **rtp:** Real-Time Transport Protocol (RTP) destination port.
- **tunnel-group**: VPN tunnel traffic. If you use this criterion, you can also configure the class to match a specific destination IP address within the tunnel group.

Class maps are assigned to policy maps.

Policy Maps

The class map determines what is matched, and the policy map associates one or more actions with a class of traffic.

The policy actions that can be configured are as follows:

- Forward the traffic flow to the Security Services Module (when present) for intrusion protection or content security and control services by creating an intrusion prevention system (IPS) or a content security and control (CSC) policy.
- Perform a specified protocol inspection or inspections by creating an inspection policy.
- Police the bandwidth used by the specified flow by creating a quality of service (QoS) police policy.
- Direct the flow to the low-latency queue by creating a QoS priority policy.
- Set connection parameters on the flows by creating a set connection policy.

Service Policies

The service policy activates a policy map on a targeted interface or globally on all interfaces. Service policies are represented as service policy rules in the ASDM.

 Please see page 110 for more details.

To configure a service policy rule, you first need to navigate to **Firewall > Service Policy Rules**. Figure 33 displays the Service Policy rules screen.

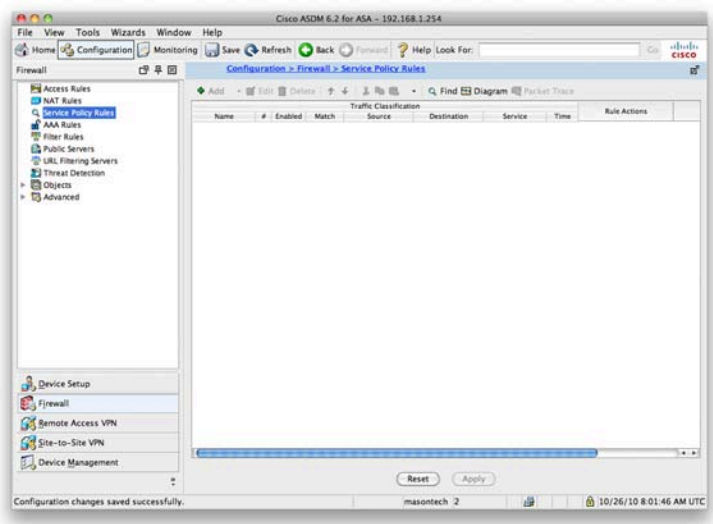
Clicking **Add** launches the Add Service Policy Rule Wizard. Three steps to this wizard configure a service policy rule:

Step 1: Configure a service policy.

Step 2: Configure the traffic classification criteria for the service policy rule.

Step 3: Configure actions on the traffic classified by the service policy rule.

FIGURE 33
Service Policy Rules

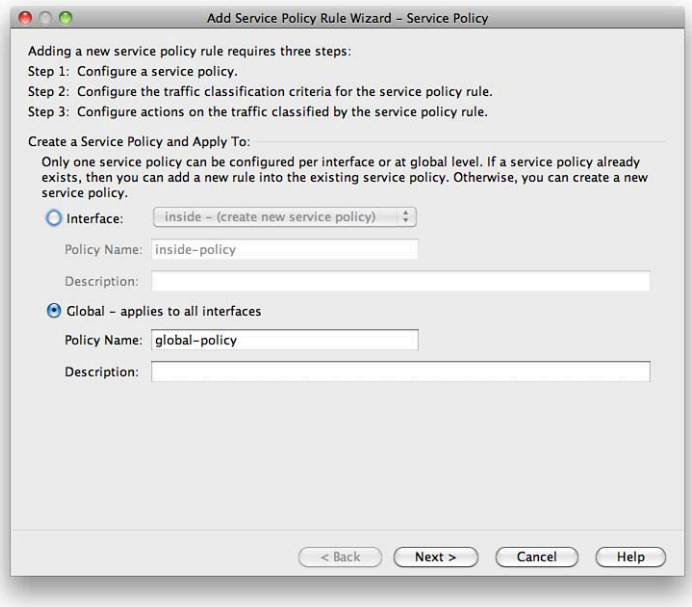


Step 1: Configure a Service Policy

In Step 1, you need to give the service policy a name and either apply it to a specific interface or apply it globally, which applies the policy on all interfaces. You can also provide a description of the service policy. You can see the screen in Figure 34.

 Please see page 110 for more details.

FIGURE 34
Service Policy Step 1



Step 2: Configure the Traffic Classification Criteria for the Service Policy Rule

You are now asked to either create a new traffic class or use an existing traffic class. When creating a new traffic class, you must enter the name for the new traffic class and supply a description. You have the option to match traffic against the criteria covered earlier in this section about class maps. This is shown in Figure 35.

When you select one of the traffic-match criteria, the next screen is the configuration screen for that criterion. You chose Tunnel Group as the traffic-match criteria, and Figure 36 shows that you have the option now to select a tunnel group to match.

 Please see page 110 for more details.

FIGURE 35
Traffic Classification

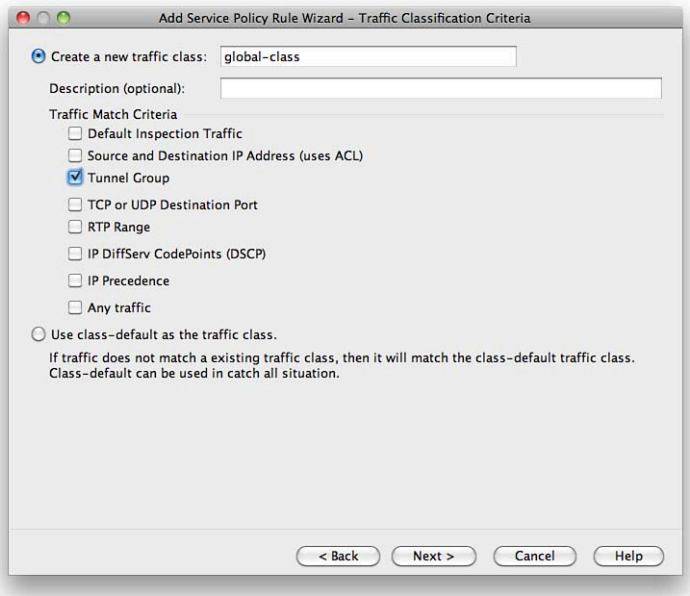
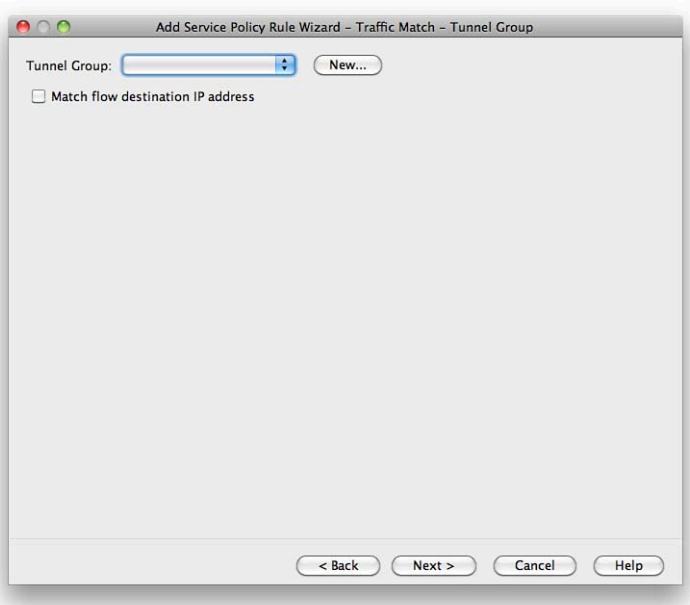


FIGURE 36
Tunnel Group



 Please see page 110 for more details.

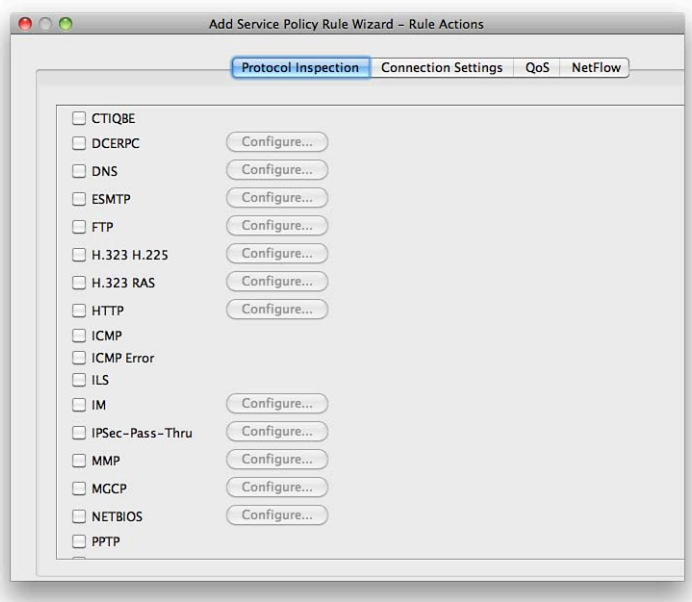
Step 3: Configure Actions on the Traffic Classified by the Service Policy Rule

The next screen is the Rule Actions screen. Three tabs display at the top of the screen:

- Protocol Inspection
- Connection Settings
- QoS

The Protocols Inspection tab enables you to configure protocol-specific inspections if the traffic-match criteria allow it, as shown in Figure 37.

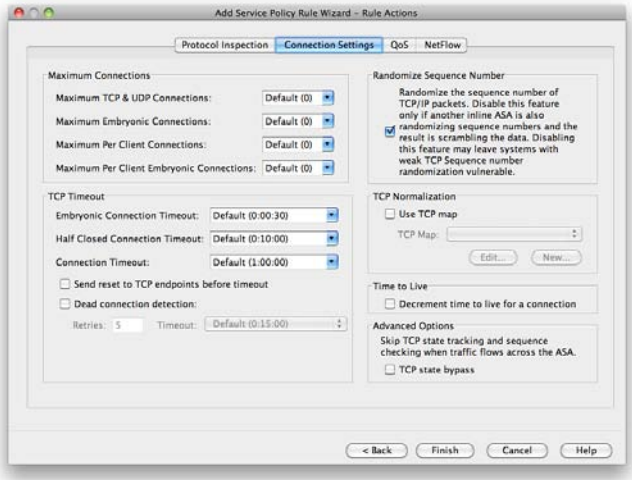
FIGURE 37
Protocol Inspection



The Connection Settings tab enables you to set the maximum connections for TCP and UDP connections and the TCP timeout. You can also choose to randomize the TCP sequence number and enable TCP normalization, as shown in Figure 38.

 Please see page 110 for more details.

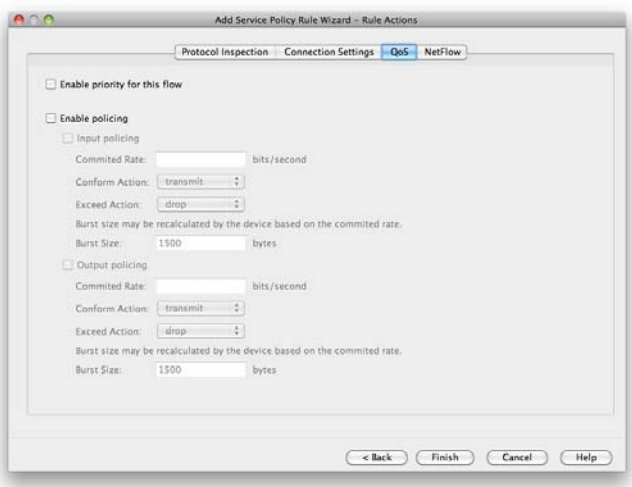
FIGURE 38
Connection Settings



You can use the QoS tab to enable priority and policing for the traffic flow. When policing is selected, you can apply QoS settings to the flow to restrict the amount of bandwidth the flow is provided when traversing the interfaces of the firewall.

You can use this setting to reduce potential denial-of-service (DoS) attempts, because you can limit the amount of bandwidth allocated to a protocol, as shown in Figure 39.

FIGURE 39
QoS



 Please see page 110 for more details.

You click **Finish** to apply the service policy rule. It is added to the ASA when you click **Apply** from the main Service Policy Rules window on the ASDM.

Application Layer Policies

The Cisco ASA Application Inspection and Control (AIC) features provide advanced application layer (OSI Layers 5 to 7) filtering that provides a more granular level of control for modern day applications.

This advanced inspection helps to prevent malicious content from being delivered to endpoints protected by the ASA that would normally bypass traditional Layers 3 and 4 Access Control Lists. AIC inspection can be performed against protocols such as HTTP, FTP, DNS, ESMTP, and other common application protocols.

The following features are provided by Application Inspection and Control (AIC) on the Cisco ASA:

- **Protocol Minimization**: Enables a minimal required set of protocol features through the ASA
- **Payload Minimization**: Enables transport of minimally required payloads over the application session
- **Application Layer Signatures**: Enables and drops known malicious payloads in application layer sessions
- **Protocol Verification**: Detects and drops anomalous application layer protocol units

Configuring HTTP Inspection

Now take a look at configuring AIC for HTTP inspection. The ASA HTTP AIC inspection can granularly parse HTTP request and responses and enable specific value and regular expression matching against this traffic. The HTTP inspector also verifies adherence to the HTTP protocol and performs URL filtering and checking against several built in HTTP signatures.

For this example configure a HTTP protection policy that filters application layer traffic from the outside to the web server previously configured that needs protecting. Create a protection policy that verifies adherence to the HTTP protocol and enables only the HTTP GET method.

 Please see page 110 for more details.

Following are two steps involved in creating the HTTP protection policy:

Step 1: Create an HTTP inspection policy map.

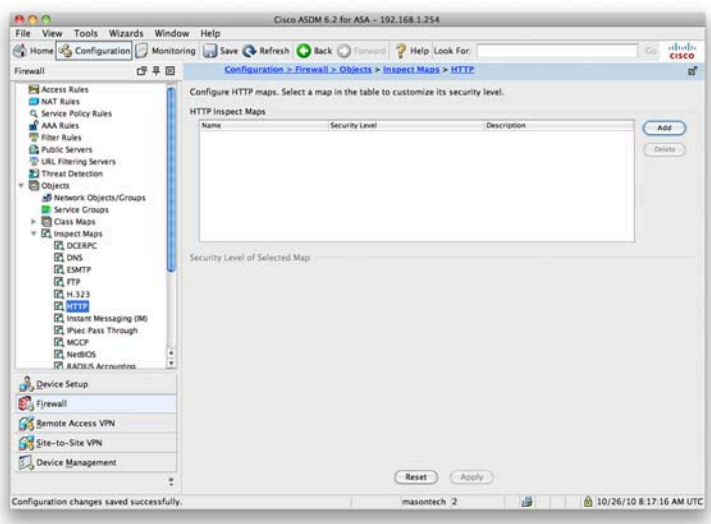
Step 2: Apply the HTTP inspection policy map.

Step 1: Create an HTTP Inspection Policy Map

You need to create the special HTTP inspection policy map to include all the inspection rules and their associated actions. The HTTP inspection policy map is the configuration container that contains a set of inspections that will be applied to a specific set of flows and is reusable in multiple traffic classes.

To create the HTTP inspection policy map using ASDM navigate to Configuration > Firewall > Objects > Inspect Maps > HTTP. This screen can be seen in figure 40.

FIGURE 40
HTTP Inspection Policy Map



Clicking Add opens a new HTTP inspection policy map. You can either use one of the built in Security Levels of Low, Medium, or High, or you can click the Details button to configure individual inspection.

For this example select the Details button to configure individual inspection for the HTTP inspection policy map.

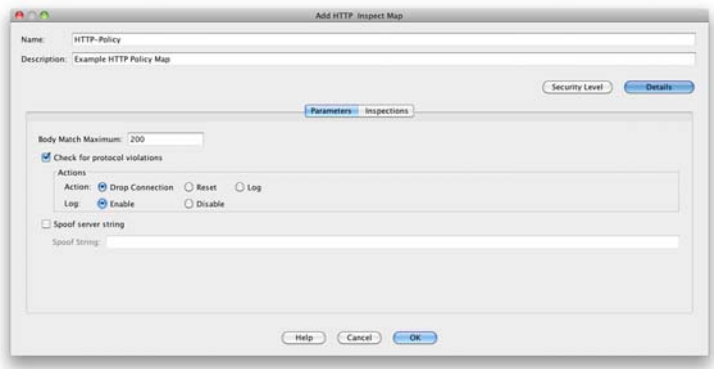
 Please see page 110 for more details.

Before you do, give the inspection policy map a name of **HTTP-Policy** and a description of **Example HTTP Inspection Policy Map**.

The first inspection to add is to implement adherence to the HTTP protocol. This is done from the Parameters tab selected by default. Ensure the Check For Protocol Violations radio button is selected, and also ensure that the traffic is getting dropped and logging is enabled.

The completed screen can be seen in Figure 41.

FIGURE 41
HTTP Protocol Adherence



To configure the next inspection, select Inspections tab to start adding the manual inspections to the HTTP policy map.

Select Add and start to configure the inspection. The first inspection to add is to allow only the GET request method HTTP protocol to the server.

In the Match Criteria section, select the Single Match option to specify a single condition. In the Match Criteria section, specify No Match as the Match Type. This drops all traffic except traffic matching the specific criteria.

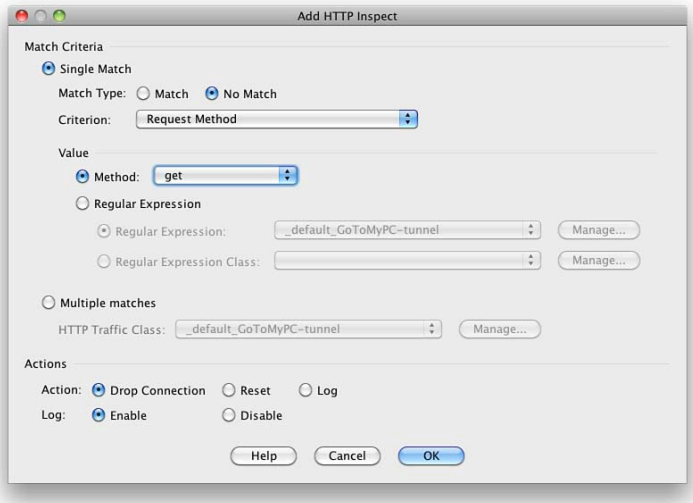
In the Criterion drop-down list, specify Request Method to filter traffic based on the HTTP request method. Select GET from the Method drop-down list.

In the Actions section, ensure that Drop Connection is chosen and ensure Logging is enabled.

 Please see page 110 for more details.

The completed screen can be seen in Figure 42.

FIGURE 42
HTTP GET method

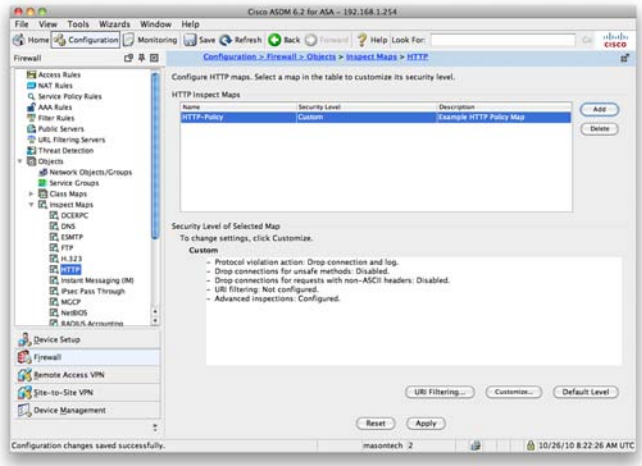


Click OK when the preceding is completed to return to the Inspection Policy Map screen.

You have now configured the HTTP inspection policy map to adhere to the HTTP protocol and enable only HTTP GET requests. The inspection policy is called HTTP-Policy and can be seen at the HTTP Inspect Maps screen, as shown in Figure 43.

 Please see page 110 for more details.

FIGURE 43
HTTP Inspect Maps



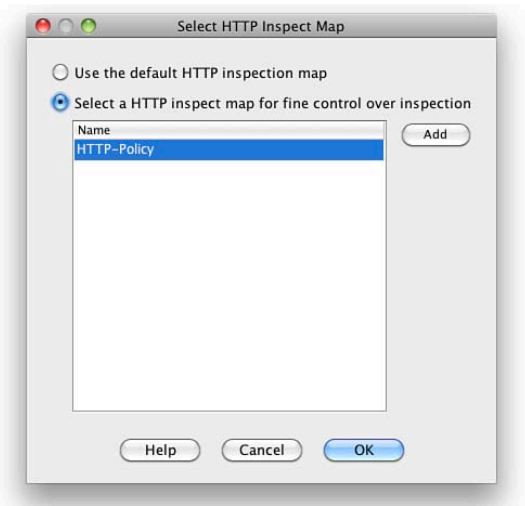
Step 2: Apply the HTTP Inspection Policy Map

In Step 1 you configured an HTTP Inspection Policy Map. The next step is to apply this policy map to the ASA so that traffic is inspected against the policy map and the correct action is taken.

The implementation of the HTTP inspection policy map is identical to the way that service policies are applied under the Modular Policy Framework covered earlier in this section.

When configuring the Service Policy rule, be sure to select the correct HTTP inspection policy map, as shown in Figure 44.

FIGURE 44
HTTP Inspection Policy Map



 Please see page 110 for more details.

NOTE
Basic threat detection is enabled by default on the ASA. There is a minimal impact on performance when there are drops or potential threats on the ASA.

Threat Detection

Threat detection on the ASA is similar in operation to an IPS.

Two types of threat detection are available on the ASA:

- Basic threat detection
- Scanning threat detection

Basic threat detection is enabled by default. You can enable both basic and scanning threat detection independently of each other. One is not dependent on the other, and therefore you can have one, both, or neither configured on your ASA.

Basic Threat Detection

The security appliance basic threat detection feature provides threat-related drop statistics by monitoring the rate of dropped packets and security events per second (eps).

When the rate of dropped packets or security events exceeds established thresholds, basic threat detection generates a syslog message.

This enables you to detect activity that might be related to an attack, such as a DoS attack.

The ASA basic threat detection provides threat-related drop statistics by monitoring the following events:

- Access list denials
- Bad packet format
- Exceeded connection limits

 Please see page 110 for more details.

NOTE
The scanning threat detection feature can significantly affect the performance and memory use of the ASA while it creates and gathers the host- and subnet-based data structure and information. Performance impact varies depending on the ASA platform.

- Detection of DoS attacks
- Failed basic firewall checks
- Detection of suspicious Internet Control Message Protocol (ICMP) packets
- Packets failing application inspection
- Interface overload
- Detection of scanning attacks
- Detection of incomplete sessions, such as TCP SYN attacks or no data UDP session attacks

The ASA tracks two types of rates for each monitored events: the average rate and burst rate. The average rate is the average rate over a time interval, and the burst rate is the one-tenth of the average rate or 10 seconds, whichever is the highest.

Syslog messages are generated when either of the rates for the monitored events is exceeded.

The following table shows the default threshold rates for basic threat detection.

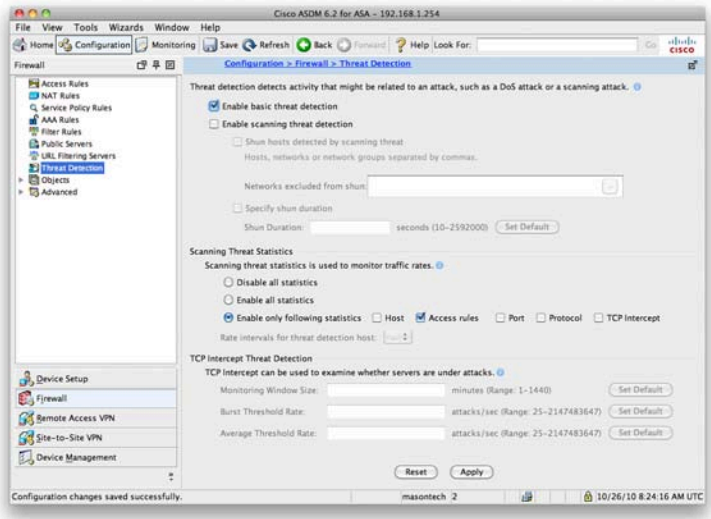
Default Threshold Rates for Basic Threat Detection

Packet Drop Reason	Average Rate	Burst Rate
DoS attack detected Bad packet format Connection limits exceeded Suspicious ICMP packets	100 drops per second over the last 600 seconds	400 drops per second over the last 10-second period
Scanning attack detected	5 drops per second over the last 600 seconds	10 drops per second over the last 10-second period
Incomplete session	100 drops per second over the last 600 seconds	200 drops per second over the last 10-second period
Denial by access list	400 drops per second over the last 600 seconds	800 drops per second over the last 10-second period
Basic firewall checks failed Packet failed application inspection	400 drops per second over the last 600 seconds	1600 drops per second over the last 10-second period
Interface overload	2000 drops per second over the last 600 seconds	8000 drops per second over the last 10-second period

 Please see page 110 for more details.

Basic threat detection is configured from the **Firewall > Threat Detection** screen. This is shown in Figure 45.

FIGURE 45
Threat Detection



You can see from Figure 45 that basic threat detection is enabled on this ASA. To disable it, uncheck the check box.

Tuning of the basic threat detection is performed in the CLI configuration with the **threat-detection** command. This is beyond the scope of the ASAF exam.

Scanning Threat Detection

The scanning threat detection feature of the ASA is concerned with hosts performing network scans against networks protected by the ASA.

Network reconnaissance scans, or port scans as they are commonly known, are normally a precursor to an attacker launching a full-blown attack on a system. The first step is normally to identify which ports and services are available on a system before enumerating and fingerprinting these ports to check for known vulnerabilities. A known vulnerability is always the preferred route in for attackers because they can use simple attack scripts to gain access and then escalate privileges.

 Please see page 110 for more details.

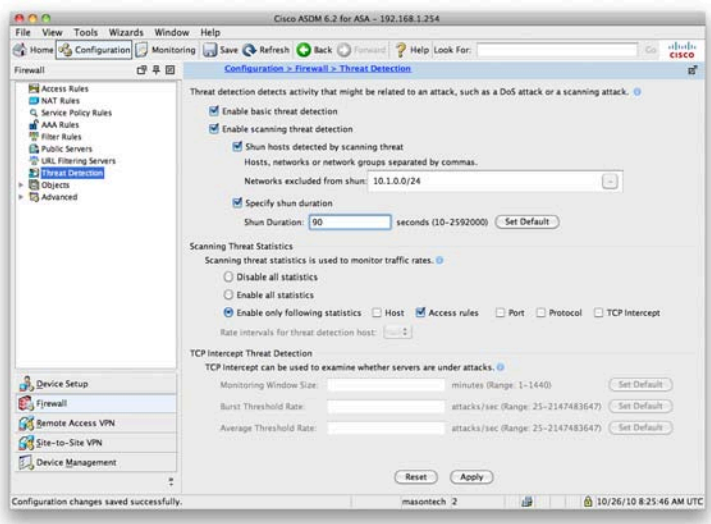
When performing scanning threat detection, the ASA uses an extensive database of host statistics to generate syslog messages when a host is identified as either an attacker, or a target.

As with basic threat detection, scanning threat detection is configured from the **Firewall > Threat Detection** screen.

You have now enabled scanning threat detection and selected to shun hosts detected by scanning threat.

Figure 46 shows the Threat Detection configuration window with both basic threat detection and scanning threat detection enabled.

FIGURE 46
Threat Detection: Basic and Scanning



When a shun is activated, all current connections from the malicious host are dropped, and all future connections are blocked at the outside interface of the ASA. Shuns are dynamic in nature and are not stored as a part of the configuration. If the security appliance loses power or reloads, any active shuns are lost.

You can specify a network, or network object, that will *not* be shunned. In the example, you set that 10.1.0.0/24 will not be shunned. This setting is useful for entering networks that should never be blocked, such as testing partners or third-party support organizations. You also set the ASA so that devices are shunned for 90 seconds.

 Please see page 110 for more details.

Summary

This section expanded on the previous section and provided a simple network that addressed the interfaces, configured NAT for outbound access, and enabled a static translation to an internal web server. You also created an access rule that enabled inbound HTTP and HTTPS traffic to the web server using an object group rather than individual access control list entries.

You then looked at more advanced topics such as the Modular Policy Framework (MPF), Application Inspection Policies (AIP), and Threat Detection.

The next section looks at integrating the ASA into your network and covers routing, switching, and operating the firewall in Transparent mode.

 Please see page 110 for more details.

Section 4
ASA Network Integration

This section covers the integration of the Cisco ASA into common networks. The ASA has many features that help with the integration into a network, and in this section you cover routing, switching, and transparent firewalling on the Cisco ASA.

Routing

The ASA supports both static and dynamic routing. Static routing is performed through a static route, and dynamic routing is enabled with a dynamic routing protocol. The ASA supports the Routing Information Protocol (RIP), Open Shortest Path First (OSPF) Protocol, and Enhanced Interior Gateway Routing Protocol (EIGRP).

Configure a Static Default Route on the ASA

One of the commonly used routes on the ASA will always be the static default route. This is the destination of last resort and where all packets are sent that do not match a more specific route on the ASA.

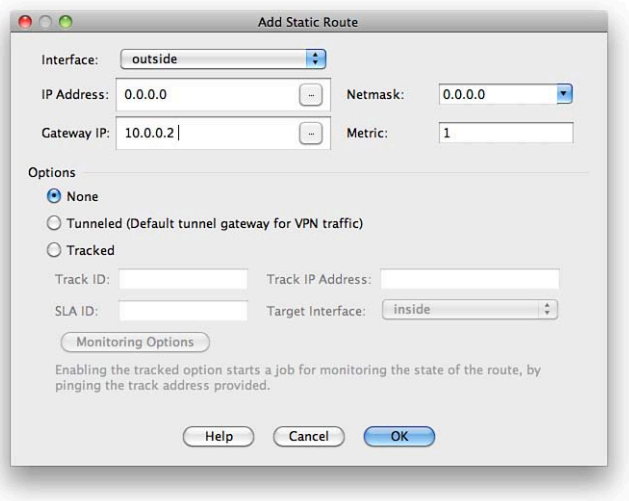
A high percentage of ASAs are deployed at the network perimeter, normally acting as the firewall between the corporate network and the public Internet. In these cases, a static default route will always be used that points out to the Internet.

To configure a static default route, select **Configuration** from the ASDM toolbar and then **Device Setup**. One of the options now presented is Routing. The first option configures static routes.

Click **Add** to add a static route. Figure 47 shows a default static route that you have entered that sends traffic to the next hop from the ASA out to the public Internet.

 Please see page 110 for more details.

FIGURE 47
Static Default Route



You can see from Figure 47 that a route is set to 0.0.0.0 0.0.0.0 that points to 10.0.0.2. The notation of 0.0.0.0 0.0.0.0 is the default catchall address, which can also be represented as 0 0.

With this static route in place, any packet sent through to the ASA that the ASA does not hold a local route for will be forwarded to 10.0.0.2. The device at 10.0.0.2 is the exit point from the network to the Internet.

Configure RIP on the ASA

The Routing Information Protocol (RIP) can be configured on the ASA. The ASA supports both RIPv1 and RIPv2. Earlier security devices such as the PIX would operate only in passive mode, in which the interfaces configured for RIP would only accept routes and not propagate routing information from the device. The ASA enables the device to participate in full RIP routing.

For this example, look at how to configure passive RIP on the ASA. RIP configuration is performed from the RIP section of the Routing navigation that is located under Configuration > Device Setup. The first step is to enable RIP on the ASA. Figure 48 shows the configuration required for RIPv2.

 Please see page 110 for more details.

FIGURE 48
RIPv2 Configuration

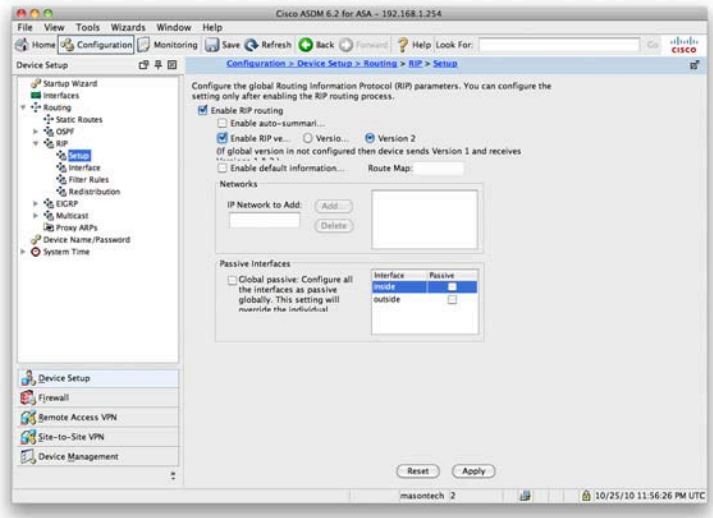
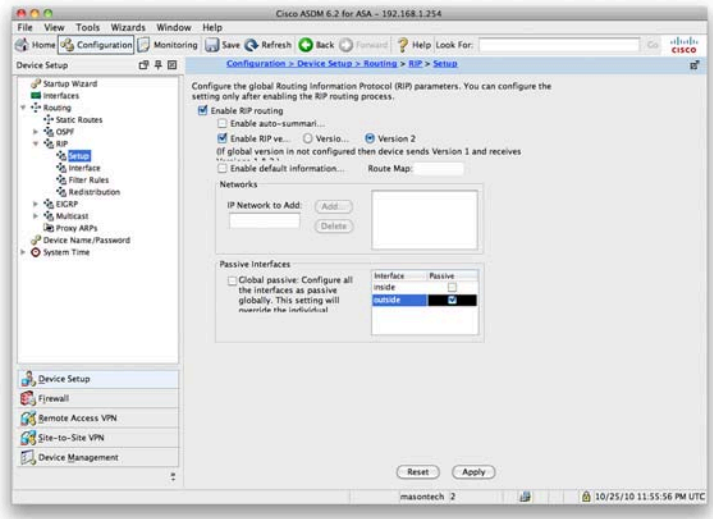


Figure 48 shows that you have enabled RIP; set it to use RIPv2. This setup configures RIPv2 on the ASA so that it fully participates in RIP routing, accepting routes from neighbors and transmitting routing updates to neighbors.

If you want to configure RIP in passive mode, just click the Passive Interfaces mode, and either select it globally, where all interfaces are put into passive mode, or select an interface. Figure 49 shows this with just the outside interface configured for passive RIP.

 Please see page 110 for more details.

FIGURE 49
Passive RIPv2 Configuration



This setup means that the ASA will listen and accept routes learned via RIP but will not advertise any of its own routes out to adjacent RIP neighbors.

Configure OSPF on the ASA

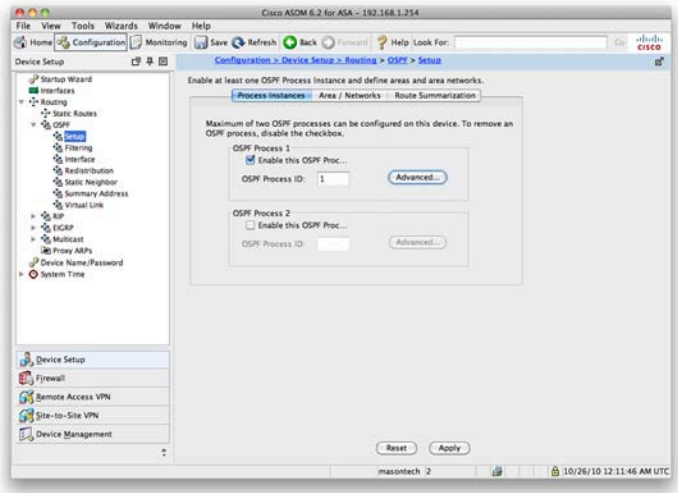
The Open Shortest Path First (OSPF) dynamic routing protocol is a much more scalable and configurable routing protocol than RIP and is often found in larger network deployments due to the scalability limitations of RIP.

The ASA supports OSPF for dynamic routing and supports up to two OSPF processes. OSPF configuration is performed from the OSPF section of the Routing navigation located under Configuration > Device Setup.

The first step in configuring OSPF is to enable the OSPF process and to enter an OSPF process ID. The process ID is only locally significant. You can see in Figure 50 that you have enabled OSPF with the process ID of 1.

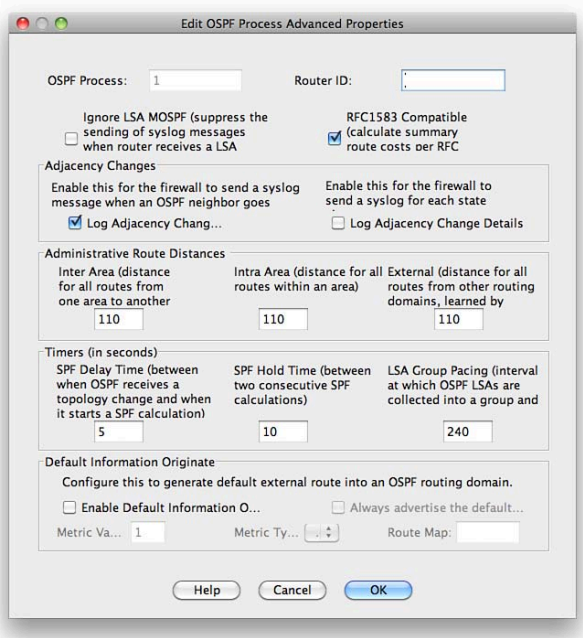
 Please see page 110 for more details.

FIGURE 50
OSPF Configuration



Clicking the Advanced tab brings up a set of configurable items for OSPF that can be seen in Figure 51:

FIGURE 51
OSPF Advanced Items

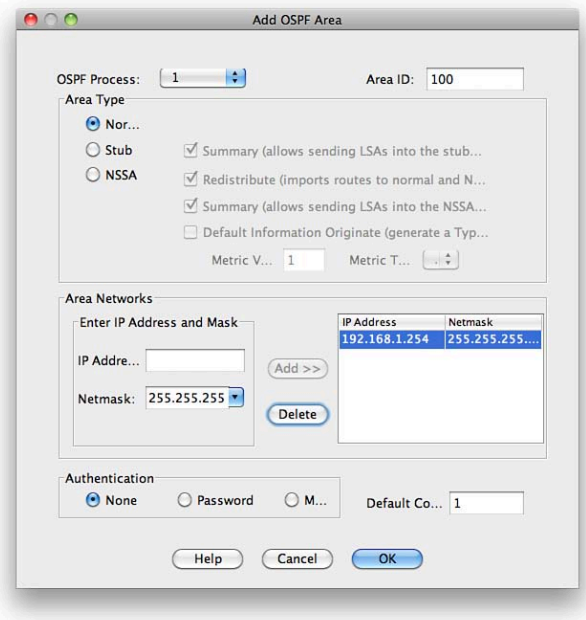


 Please see page 110 for more details.

Click OK to leave these as they are and return back to the OSPF setup screen. The next step is to configure the OSPF areas and to place interfaces within an OSPF area. Use OSPF area 100, and place the inside network interface with the IP address of 192.168.1.254 in this area.

Figure 52 shows that Area 100 is configured against OSPF process ID 1, and the IP address of 192.168.1.254 is added into this area.

FIGURE 52
OSPF Area Configuration



Clicking Apply confirms and applies this configuration to the ASA. OSPF is now configured for area 100 on the ASA.

 Please see page 110 for more details.

Switching

NOTE
You cannot configure subinterfaces on the ASA 5505 because it is a switch-based appliance where the eight physical interfaces are part of the switch and must be assigned to a VLAN interface.

The ASA enables you to configure multiple logical interfaces connected to a single physical interface. Therefore, you can assign the logical interfaces to specific VLANs.

These logical interfaces are called subinterfaces. You can assign only a single VLAN to a subinterface. Each subinterface must have a VLAN ID before it can pass traffic. Because VLANs enable you to keep traffic separate on a given physical interface, you can increase the number of interfaces available to your network without adding additional physical interfaces or security appliances. Therefore, you can use the ASA in areas that require more interfaces than exist on the installed ASA.

When a physical interface is split into subinterfaces, the physical interface becomes an 802.1Q trunk. This is the same concept as when a switch port on a Cisco Catalyst switch is configured as a trunk to pass VLAN traffic between switches.

The following table shows the maximum number of physical and logical interfaces that you might configure per an ASA model.

Maximum Number of Interfaces

ASA Model	Physical Interface	Logical Interface
ASA 5505	8	3 (20*)
ASA 5510	3 (5*)	50 (100*)
ASA 5520	5	150
ASA 5540	5	200
ASA 5550	13	250
ASA 5580	10	100

* Indicates with the Security Plus license

 Please see page 110 for more details.

To configure a logical interface, you must add an interface from the Add Interface screen, as shown in Figure 53

FIGURE 53
Creating a Subinterface

You can then select which interface this subinterface is to be bound to and set the options such as the VLAN ID and subinterface ID to configure the subinterface.

Transparent Firewalling

The Cisco ASA can operate in two modes: routed and transparent. Routed mode is the default mode, and this is where the ASA acts as a Layer 3 device, requiring an IP address on each interface from a different Layer 3 subnet. The ASA in routed mode operates like a router and makes the firewalling decisions while the packets traverse from one ASA interface to another ASA interface.

 Please see page 110 for more details.

Transparent mode is where the ASA acts like a Layer 2 bridge. In transparent mode the ASA is based on MAC addresses, and it will no longer sit on the perimeter between subnets; instead, it acts as a transparent bridge. An ASA running in transparent mode differs from routed mode in the following ways:

- Supports only two interfaces
- Requires only one IP address
- Bridges packets from one interface/VLAN to the other
- Performs MAC address lookups rather than routing table lookups
- Passes traffic that cannot be passed by a security appliance in routed mode

The following are limitations that you must consider when implementing an ASA in transparent mode:

- Dynamic DNS is not supported.
- Dynamic routing protocols are not supported.
- IPv6 is not supported.
- DHCP Relay is not supported.
- QoS is not supported.
- Multicast is not supported.
- Virtual private network (VPN) termination is not supported.

One of the main advantages of using an ASA in transparent mode is that you can place the ASA in the network without re-addressing. This makes the firewall a viable solution in which the infrastructure already exists, and re-addressing would prove troublesome.

 Please see page 110 for more details.

Now look at how to configure the ASA as a transparent firewall. The initial configuration change from Routed to Transparent mode is made using the CLI, and then the further configuration of the ASA in Transparent mode is made using the ASDM.

NOTE
When switching modes between routed and transparent, the ASA clears the configuration. Therefore, it is important that you have a backup of the current configuration. The ASA provides no warning or no confirmation, so this command can be dangerous if used incorrectly. So, you should also change the mode while connected via the console cable. A Secure Shell (SSH) or Telnet connection to the ASA can result in a loss of connection if the firewall mode is changed.

Transparent Firewall Configuration: CLI

From the command line, you can verify what the current firewall mode is with the **show firewall** command:

```
ciscoasa# show firewall
     Firewall mode: Router
```

This shows that the current firewall is in routed mode. You can switch the ASA to Transparent mode with the following command:

```
ciscoasa# configure terminal
     ciscoasa(config)#firewall transparent
```

Checking the current firewall mode now shows the following:

```
ciscoasa# show firewall
     Firewall mode: Transparent
```

The ASA is now in transparent mode. If you check the running configuration, you can see that all the interfaces will be in a shutdown state, with the entire VLAN, interface, and IP configuration that you have previously entered absent.

The first configuration step with Transparent mode is to assign the management IP address. Because the ASA does not now participate in IP routing, you need to give the ASA an IP address so that you can access it via SSH and the ASDM for management.

Use the same IP address as before, 192.168.1.254, but this time it will be as the management IP address. Configure this with the following command.

```
ciscoasa(config)# ip address 192.168.1.254 255.255.255.0
```

 Please see page 110 for more details.

This sets the management IP address to be 192.168.1.254/24. You can use the show ip address command to verify this:

```
ciscoasa# show ip address
Management System IP Address:
        ip address 192.168.1.254 255.255.255.0
Management Current IP Address:
         ip address 192.168.1.254 255.255.255.0
```

You now need to configure the two interfaces to use with the ASA. For ease of use, call these the default inside and outside interfaces, as covered in Section 2, "Basic Connectivity and Device Management."

Note that although the inside and outside interfaces are on the same subnet, they have to be on different VLANs; otherwise, the ASA will not pass traffic. Figure 54 shows the change to the topology that you are using so that the ASA in your example will be used in Transparent mode.

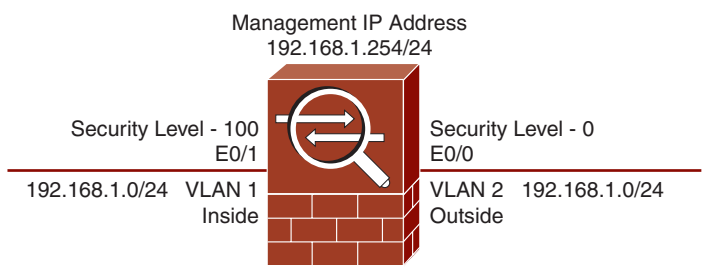


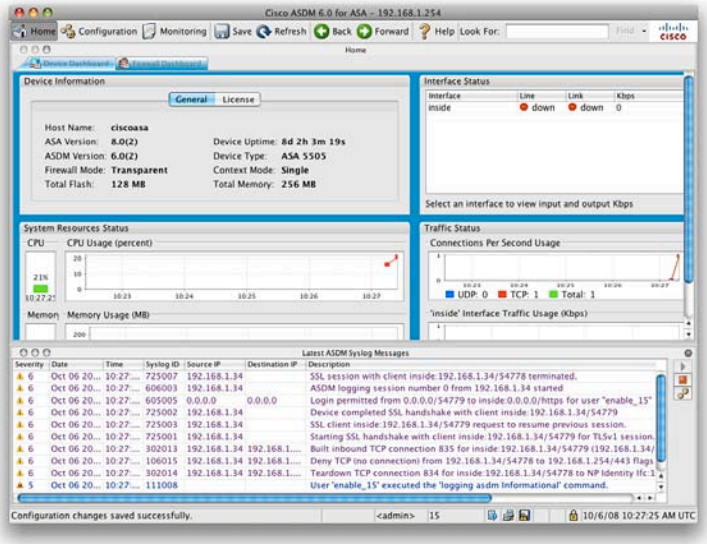
FIGURE 54
Transparent Mode Topology

You now need to follow the steps outlined in Section 2 to set up the ASA so that you can access ASDM. In brief, enable and configure an interface, and enable the HTTP server on the ASA. When that is completed, you can connect to the ASDM using the 192.168.1.254 management address that you configured.

Figure 55 shows being connected again to the ASDM. Notice that the firewall mode is shown as transparent.

 Please see page 110 for more details.

FIGURE 55
ASDM: Transparent Mode



Now configure the transparent firewall in ADSM.

If you need to switch back to router mode, you must use the **no firewall transparent** command to return to the original routed mode of the ASA:

```
ciscoasa(config)# no firewall transparent
```

Checking the current firewall mode now shows the following:

```
ciscoasa# show firewall
    Firewall mode: Router
```

Transparent Firewall Configuration: ASDM

After you connect to the ASDM, you can notice that some of the configuration options available when the ASA was in routed mode are not available any more.

When the ASA is in transparent mode, there is limited functionality and new functionality such as the ability to create

 Please see page 110 for more details.

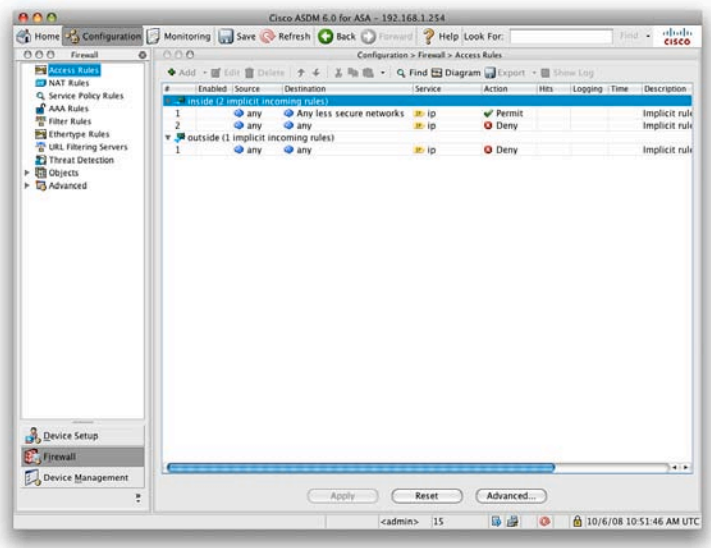
Ethertype rules. Adding an access rule on a transparent firewall is the same as adding an access rule on a routed firewall. You do it from the **Firewall > Access Rules** screen, and the format is the same for a transparent ASA as for a routed ASA.

Figure 56 shows the default access rules for the ASA in Transparent mode.

Note that these default rules are the same as with a routed ASA. Therefore, the Adaptive Security Algorithm still applies to the security level, enabling traffic to flow only in one direction by default (without the addition of access rules to permit it).

Now look at two functions that you can perform with the ASA in Transparent mode that you cannot do in Routed mode. These are permitting multicast and broadcast traffic through the ASA and configuring an Ethertype ACL.

FIGURE 56
Access Rules: Transparent Mode



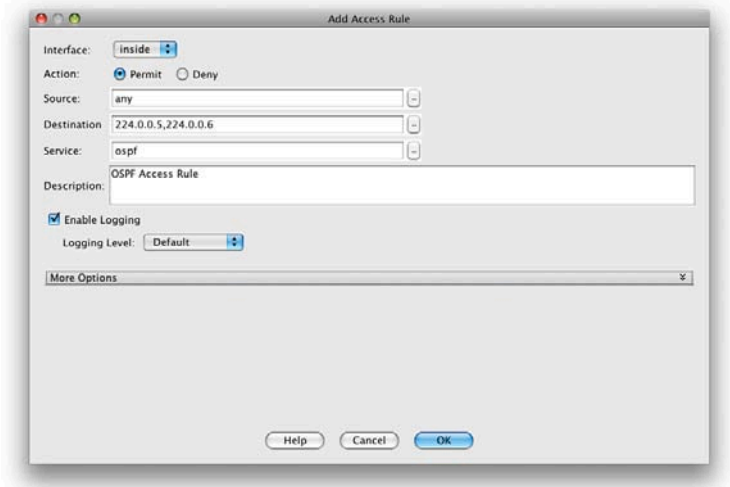
Permitting Multicast and Broadcast Traffic

Because the ASA is now operating as a bridge, you can pass multicast and broadcast traffic through it. This is good for passing traffic such as dynamic routing protocols, DHCP, and multicast streams, all of which cannot pass through a traditional routed ASA.

 Please see page 110 for more details.

Now create an access rule to permit Open Shortest Path First (OSPF) Protocol traffic through the ASA in both directions. OSPF uses multicast addresses to communicate with its neighbors and to send routing updates. Figure 57 shows an access rule that enables any traffic destined for the multicast address 224.0.0.5 or 224.0.0.6.

FIGURE 57
OSPF Access Rule



Then create a rule on the outside interface to enable OSPF to be allowed from the outside in. When this is applied, you are presented with the Access Rules screen, as shown in Figure 58.

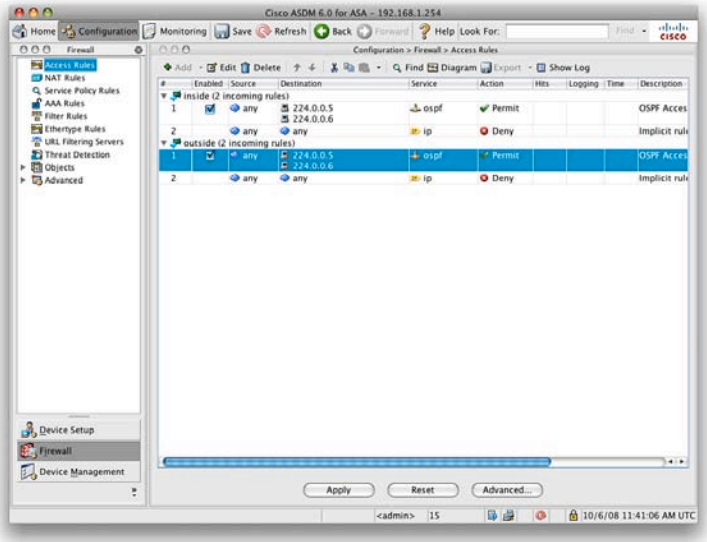
Configuring an Ethertype ACL

When the Cisco ASA is in Transparent mode, it can also allow non-IP traffic through the firewall, something that the ASA in Routed mode could not do. This is achieved by creating an Ethertype ACL.

Layer 2 traffic has an Ethertype that can be seen in the Layer 2 headers of the frame. These Ethertypes are assigned by the Internet Assigned Numbers Authority (IANA), and the list of assigned Ethertypes can be downloaded from **http://www.iana.org/assignments/ethernet-numbers**.

 Please see page 110 for more details.

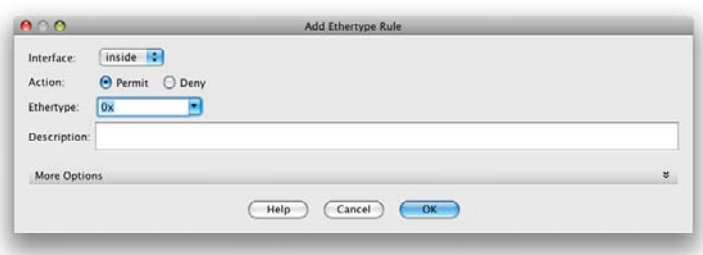
FIGURE 58
Access Rules Screen Showing OSPF



To configure an Ethertype rule, navigate to **Firewall > Ethertype Rules**. From here, you can add a new rule.

Figure 59 shows the Add Ethertype Rule window. From here, you can select the interface, action, and Ethertype to permit or deny.

FIGURE 59
Ethertype Rules



 Please see page 110 for more details.

The common supported Ethertypes on the ASA are as follows:

- BPDU
- IPX
- MPLS-Multicast
- MPLS-Unicast

In addition to these built-in Ethertypes, you can enter any value for any Ethertype, as outlined in the IANA Ethertype assignments. The value must be entered in hexadecimal format. For example, ARP would be 0x0806.

Verifying the Transparent Firewall

From the CLI, you can use a few commands to verify the transparent firewall. Some of the main ones are listed here:

- **show firewall**: Displays the mode the firewall is in
- **show access-list**: Displays the currently configured access lists
- **show mac-address-table**: Displays the bridging MAC address table
- **show arp**: Displays the Address Resolution Protocol (ARP) table of the ASA

Summary

This section looked at integrating the Cisco ASA into your existing network. The ASA requires to be integrated within your network, and one of the first configuration items you need to perform is to ensure the ASA can route traffic to its intended destination. This section looked at static routing before moving onto covering dynamic routing and the configuration of both the Routing Information Protocol (RIP) and the Open Shortest Path First (OSPF) protocol.

Switching with the ASA was then covered before moving onto transparent firewalling where the main mode of the ASA is changed so that it operates transparently as a Layer 2 firewall within an existing network.

In the next section you look at how Authentication, Authorization, and Accounting can be configured on a Cisco ASA.

 Please see page 110 for more details.

Section 5
AAA Configuration on the Cisco ASA

Authentication, Authorization, and Accounting, also known as AAA, are three services common to most Cisco devices. They are core networking services and are related to individual users whom access a system.

The first thing you want to do is *authenticate* your users to see whom they are and to ensure they are allowed to connect to the system. After you have authenticated the users, you can then *authorize* them to perform specific activities (so that all users do not have the same access rights on the system). You might also want to enable *accounting* to record what your users are doing on the system; you can log such items as logon and logoff times and any commands entered if they are connected in-line to a device.

Authentication protocols provide the AAA services. The two authentication protocols used in Cisco environments are TACACS+ and RADIUS. Both TACACS+ and RADIUS can be used on the Cisco ASA for AAA services.

Authentication: Who Is That User on the System?

Authentication is the process of identifying users on the system. This is the username and password identification that you are so familiar with.

Three types of authentication are supported on the Cisco ASA:

- **Security appliance console access**: Access to the security device through a protocol such as Telnet or SSH.
- **Cut-through proxy**: Requires user authentication for a session through the ASA. Successful authentication enables access through the ASA to specific resources.
- **Tunnel access**: For authenticating remote VPN users within a VPN tunnel to provide an extra level of security.

 Please see page 110 for more details.

Authorization: What Privileges Does the User Have?

Authorization occurs after authentication. Users have to be first authenticated to be authorized. Authorization is provided to restrict what authenticated users can do on the ASA and through resources offered by the ASA.

- **Security appliance console access**: Lets you control what commands authenticated users can issue on the ASA.
- **Cut-through proxy**: Apply ACLs to authenticated users using the cut-through proxy service of the ASA.
- **Tunnel access**: The remote VPN users can have a series of rules enforced on them when authenticated, including VPN access hours, simultaneous logons, client block rules, personal computer firewall type, idle timeout, and so on. The tunnel user or group information is applied to the tunnel before the tunnel is fully established.

Accounting: What Has the User Done?

When authenticated, the user's activity can be tracked; this is called accounting. Activity such as logging on to the ASA or using the cut-through proxy service can be recorded, as can which configuration commands have been entered for users authenticated against the security appliance console access.

AAA Configuration

Now turn your attention to using the ASDM to configure AAA services on the ASA. The first thing to consider when configuring AAA services is the user database. Two main types of user databases can be used in the configuration of AAA: the local user database and an external user database.

Local User Database Configuration

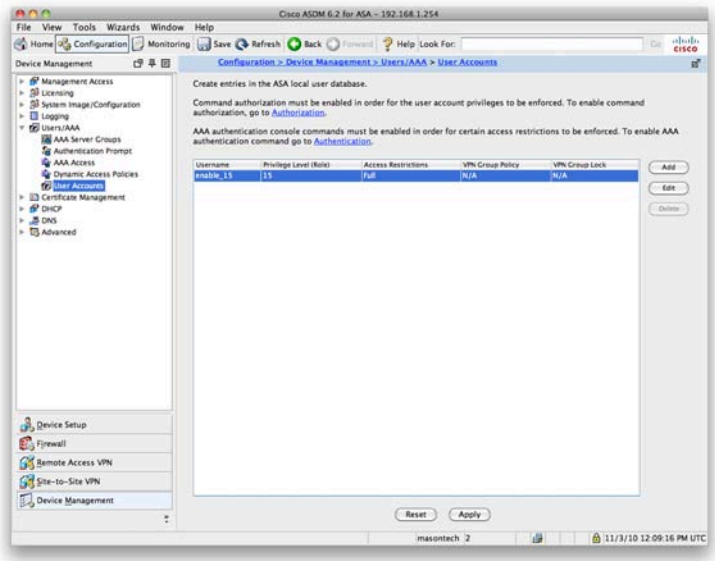
The ASA comes with the built-in capability to store user account information in an internal database, the local user database. This database is used when an external user database is not available or as a backup in case the external user database were to fail or not be reachable from the ASA.

 Please see page 110 for more details.

By default, a single default user is created in the local account database: the user called enable_15.

Figure 60 shows the default User Accounts screen that you can access by selecting **Configuration** on the toolbar and then **Device Management > Users/AAA > User Accounts**.

FIGURE 60
Default User Accounts



NOTE
The minimum password length is 4 characters, and the maximum is 32 characters (recommended = 8). Passwords are case-sensitive. When you enter a password, the Password field displays only asterisks.

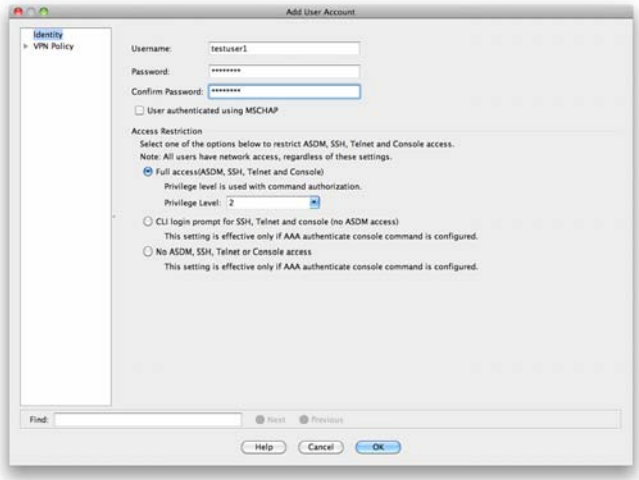
To enter a user into the local user database, click **Add**. The Add User Account screen opens.

Now add a user called testuser1 to the local account database. Enter the username **testuser1** into the Username field. Enter the password **cisco123** into the Password field.

Confirm the password, and then click **OK** to add the user to the local user database. You can see the completed Add User Account screen in Figure 61.

 Please see page 110 for more details.

FIGURE 61
Add User Account

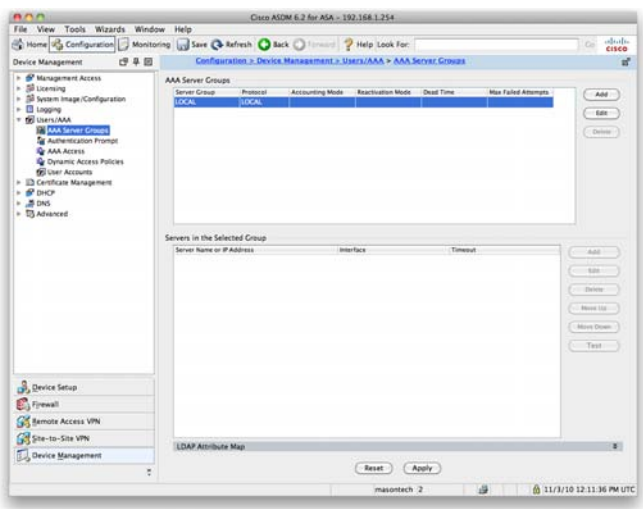


You now have two users in the local user database: the default enable_15 user, and the newly created testuser1. The user enable_15 has a privilege level of 15, and you can see that the testuser1 has a privilege level of 2.

You can set a local user lockout policy so that the user account locks after a maximum number of failed authentication attempts. This lockout is a useful security feature that helps prevent dictionary and brute-force attacks against user accounts.

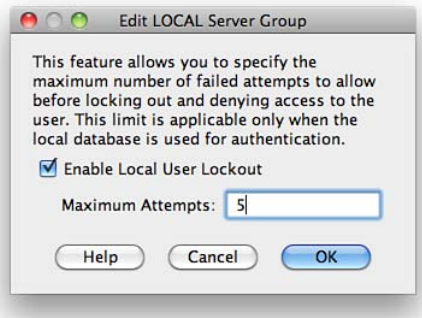
To configure the local user lockout, navigate to the **Device Management > Users/AAA > AAA Server Groups** screen (see Figure 62).

FIGURE 62
AAA Server Groups



From this screen, you can see that the only created AAA server group is the LOCAL group. Click **Edit**, and the Edit LOCAL Server Group window appears (see Figure 63).

FIGURE 63
Edit LOCAL Server Group

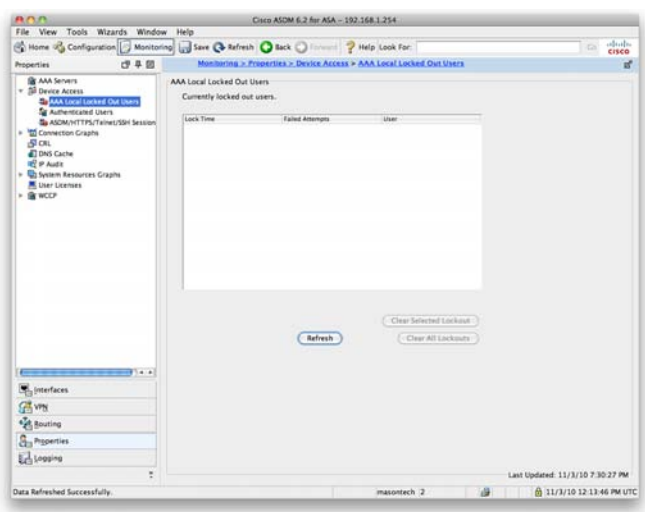


Click to enable local user lockout, and set the maximum attempts to 5, as shown in Figure 63.

At this point, you have just enabled local user lockout. If a user gets his password wrong five times in a row, his account is locked. The user account has to be manually unlocked. You can unlock it from the AAA Local Locked Out User screen available by choosing **Monitoring** from the toolbar and then navigating to **Properties > Device Access > AAA Local Locked Out Users**.

Figure 64 shows the AAA Local Locked Out Users screen.

FIGURE 64
AAA Local Locked Out Users



 Please see page 110 for more details.

To reenable a locked account, select the locked-out account, and then click the **Clear Selected Lockout** button.

External User Database Configuration

The second type of authentication database is an external user database. This is a database that sits external from the ASA.

The ASA supports the following external user databases:

- RADIUS
- TACACS+
- Microsoft Windows NT domain
- SDI
- Kerberos
- LDAP
- HTTP Form

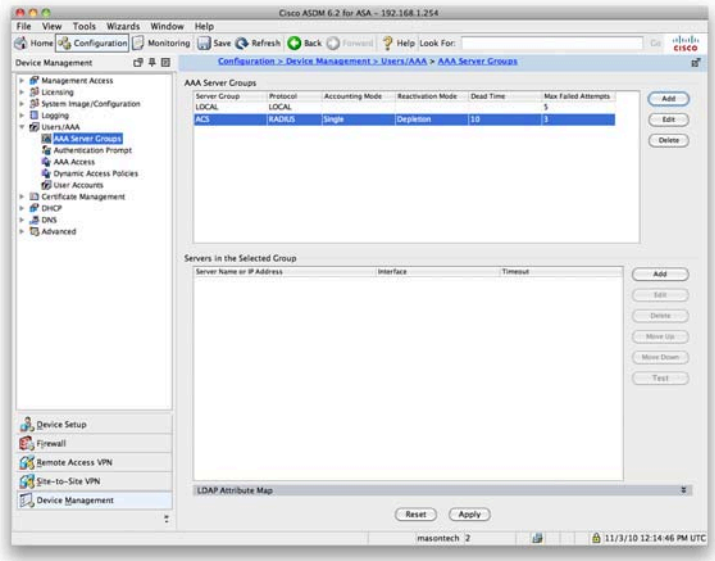
Cisco Access Control Server (ACS) is a software application for Windows or UNIX that provides RADIUS and TACACS+ authentication protocols. Cisco Secure ACS is also available as an appliance that exists on a prebuilt server and can be treated as a true authentication appliance. To use an external user database, you must define the AAA server group and then add the authentication servers into the group.

Navigate to the **Device Management > Users/AAA > AAA Server Groups** screen. You should just see the default LOCAL server group. Add a new server group called **ACS** and select the defaults.

You now have the groups LOCAL and ACS (see Figure 65).

 Please see page 110 for more details.

FIGURE 65
AAA Server Groups



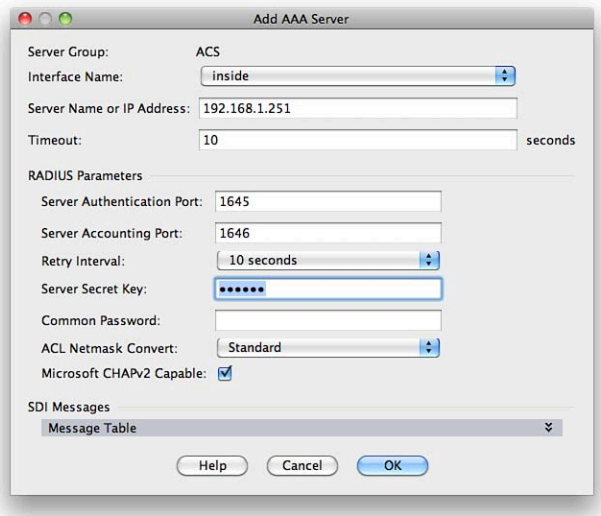
You now need to add a server to the group. Ensure the ACS group is highlighted, and then click **Add** under Servers in the selected group.

In the example, you configure access to a RADIUS server on the inside interface with an IP address of 192.168.1.251. You have to set a server secret key that is also configured on the ACS server to authenticate it against the ASA.

Figure 66 shows the Add AAA Server screen

 Please see page 110 for more details.

FIGURE 66
Add AAA Server



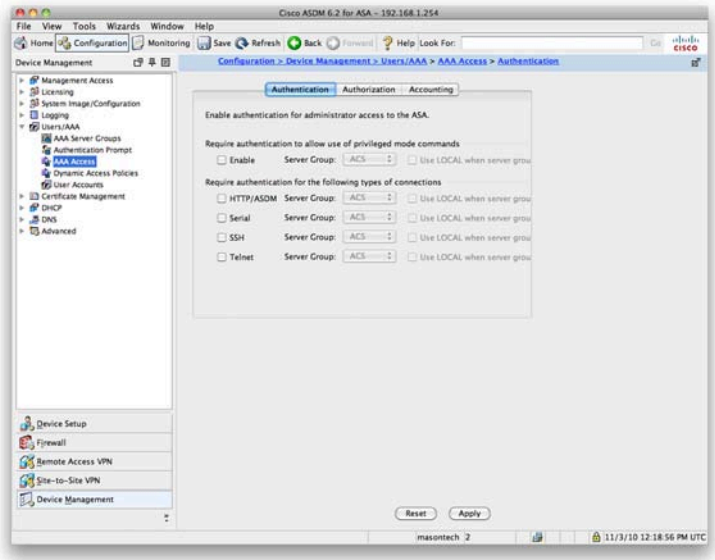
You now have the ACS AAA server group and the single server in that group. You can have multiple servers in a group for redundancy and for load balancing when the network is heavily used.

To enable authentication against the AAA server that you have just added, you need to navigate to the **Device Management > Users/AAA > AAA Access** screen. From this screen, you can enable AAA for the server group that you just created.

Figure 67 shows the AAA Access screen and the configuration options on the Authentication tab.

 Please see page 110 for more details.

FIGURE 67
AAA Access Screen



Auth-Proxy Configuration

NOTE
Authentication proxy is also known as auth-proxy and cut-through proxy. The feature is also available on the PIX, IOS Firewall, and other leading security vendors.

The authentication proxy is where the ACS prompts the user for authentication against a specific service on the initiation of the session, and then after successful authentication, the user is authorized to use the services for a determined time period without reauthentication or reauthorization.

The ASA supports the following protocols for authentication proxy:

- TCP Port 21 for FTP
- TCP Port 23 for Telnet
- TCP Port 80 for HTTP
- TCP Port 443 for HTTPS

To configure authentication proxy on the ASA, you must complete three steps:

 Please see page 110 for more details.

Step 1 Specify a AAA server group.

Step 2 Designate an authentication server.

Step 3 Enable authentication proxy user authentication by configuring a AAA authentication rule.

Specify a AAA Server Group

The first step in authentication proxy configuration is to specify a AAA server group. You already configured a AAA server group called ACS that you can use for this example. Figure 65 shows the ACS server group.

Designate an Authentication Server

The second step in authentication proxy configuration is to configure an authentication server within the authentication group that you have just created. This authentication server is where the authentication will be carried out for the cut-through proxy. We already added an authentication server at 192.168.1.251, as shown in Figure 66.

Enable Authentication Proxy User Authentication by Configuring a AAA Authentication Rule

The third and last step in authentication proxy configuration is to create an AAA authentication rule that will enable authentication proxy. To do this, you must navigate to **Firewall > AAA Rules**.

By default, no AAA rules are configured. You need to add an authentication AAA rule to enable authentication proxy. First select the Add button, and then select Add Authentication Rule to be taken to the Add Authentication Rule screen.

Create an authentication rule to authenticate traffic from anywhere by going to the web server you previously created. Now authenticate on the webaccess group that you created earlier, which contains both HTTP and HTTPS.

Figure 68 shows the completed Add Authentication Rule screen.

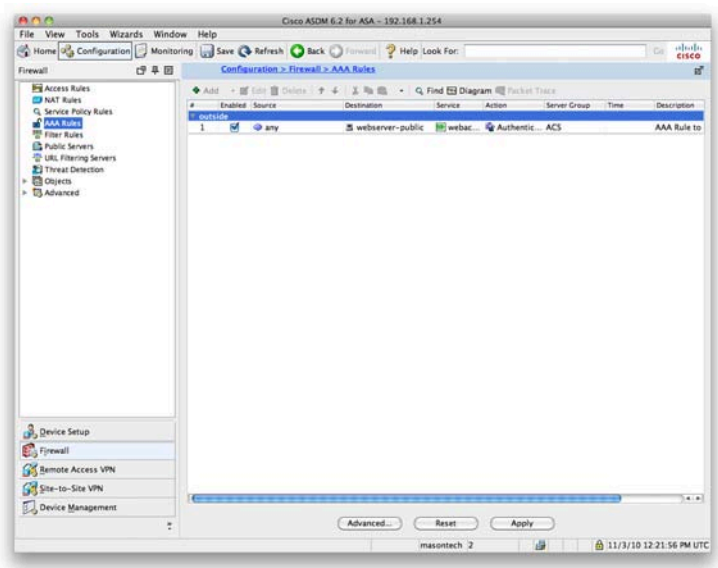
 Please see page 110 for more details.

FIGURE 68
Add Authentication Rule

In this example, after the authentication rule is applied, users are prompted for a username and password when they start HTTP or HTTPS connections to 10.0.0.5 from the outside. The AAA server verifies whether the username and password are correct. If they are correct, the security appliance cut-through proxy permits further traffic between the initiating host and the target host.

Figure 69 shows the AAA Rules screen with the applied authentication rule.

FIGURE 69
Add Rules Screen



 Please see page 110 for more details.

Summary

This section covered Authentication, Authorization, and Accounting (also known as AAA, or the triple-A services) on the ASA. You started with an overview of the roles for AAA before moving on and discussing how to configure a local user database and remote-user database.

You ended this section by seeing how to configure the authentication proxy service on the ASA. This service enables the ASA to dynamically permit or deny user access to a service based on authentication credentials, and it offers another useful layer of security between the network and the users.

In the next section, you look at configuring High Availability on the Cisco ASA.

 Please see page 110 for more details.

Section 6
ASA High Availability

This section looks at configuring the ASA for high availability. Due to the nature of the ASA, a single deployment can be also considered a single point of failure. A failure of the ASA would either prevent access to resources that the ASA is protecting or would prevent internal users from accessing an external resource such as the Internet.

Although many smaller organizations take this risk, the ASA does support virtualization and high availability demanded by larger enterprises and provides fault tolerance if a link or device failure of the ASA occurs.

ASA Failover

Failover provides redundancy for the ASA if hardware of software failure occurs. The ASA supports two types of failover:

- Hardware failure
- Stateful failover

Hardware failover provides redundancy in case of a hardware failure. This is achieved with another ASA that acts as a standby unit to take over from the primary ASA if a failure occurs. With hardware failover, the connections are dropped, and clients much reestablish their sessions.

Stateful failover passes per-connection state information from the active to the standby unit. If a failure occurs, the state table is on the standby unit, and most client applications would not require reconnecting. This should offer transparency to the end user.

Following are two modes of operation for failover, this section covers both:

- Active/standby failover
- Active/active failover

 Please see page 110 for more details.

Failover Links

To facilitate failover, the ASAs participating in failover pass between themselves information about the state of each device. Following are two types of failover links:

- LAN-based failover links
- Stateful failover links

With LAN-based failover links, the failover messages are transferred over Ethernet connections. LAN-based failover links provide message encryption and authentication using a manual preshared key for added security. LAN-based failover links require an additional Ethernet interface on each ASA to be used exclusively for passing failover communications between two security appliance units.

The stateful failover interface passes per-connection stateful information to the standby ASA unit. Stateful failover requires an additional Ethernet interface on each security appliance with a minimum speed of 100 Mb/s to be used exclusively for passing state information between the two ASAs. The LAN-based failover interface can also be used as the stateful failover interface.

Failover Requirements

To successfully configure failover, some requirements must be met:

- ASAs must be the same model number and hardware configuration.
- The same Security Service Modules must be installed.
- Before version 7, the same software version must be used.
- The same operating mode must be used.
- The same features (DES or 3DES) must be used.

 Please see page 110 for more details.

- The same amount of flash memory and RAM must be used.
- The proper licensing to support failover must be used.

Active/Standby Failover Configuration

Active/standby failover is where one ASA acts as the active or primary firewall, and the other device acts as the secondary or standby firewall. The primary ASA and secondary ASA communicate to each other over the configured interfaces and over the LAN-based failover link. The primary ASA is active and passes traffic. If a failure occurs, the secondary ASA becomes active and passes traffic on behalf of the primary ASA.

Now look at how to configure active/standby failover on a pair of ASAs using the ASDM.

Following are the five steps to this configuration:

Step 1: Cable the interfaces on both security appliances.

Step 2: Prepare both ASAs for configuration with ASDM.

Step 3: Use the ASDM High Availability and Scalability Wizard to configure the primary ASA for failover.

Step 4: Verify that Cisco ASDM configured the secondary security appliance with the LAN-based failover command set.

Step 5: Save the configuration of the secondary security appliance to flash memory.

The requirements for failover must be met before you can start this configuration. Without the correct licensing, you cannot complete the configuration.

 Please see page 110 for more details.

Step 1: Cable the Interfaces on Both Security Appliances

Cable the interfaces on both of the ASAs so that the corresponding interfaces are on common networks.

Figure 70 shows a sample cabling setup for an active/standby failover environment.

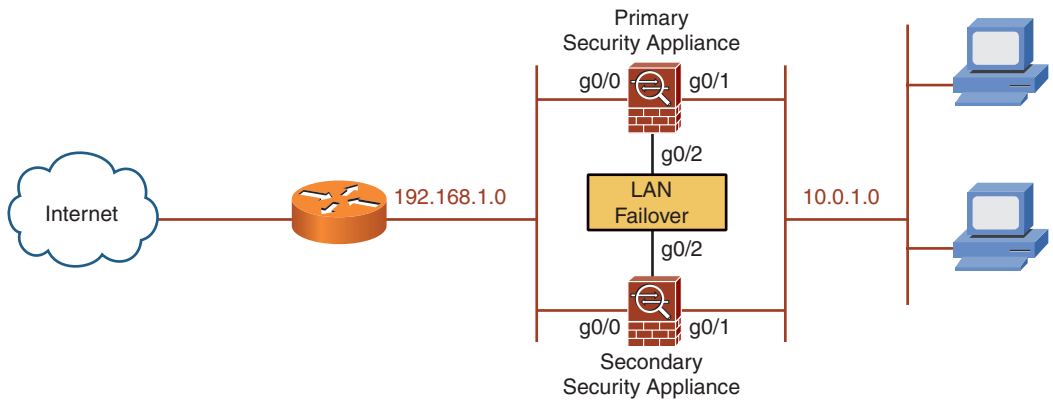


FIGURE 70
Simple firewall setup

As shown in Figure 70, a LAN-based failover connection is required between the primary and secondary ASA. If you plan to use stateful failover, an interface on the ASA must be dedicated to this function, unless you configure stateful failover to share the same interface as the LAN-based failover connection.

Step 2: Prepare Both ASAs for Configuration with ASDM

Prepare both ASAs for ASDM configuration. Section 2, "Basic Connectivity and Device Management," of this Quick Reference guide covered how to configure the ASA so that you can access it using ASDM.

Both the primary and secondary ASAs require an IP address be assigned on the inside interface that can be accessed via ASDM.

 Please see page 110 for more details.

Step 3: Use the ASDM High Availability and Scalability Wizard to Configure the Primary ASA for Failover

Configure active/standby failover using the High Availability and Scalability Wizard on the ASDM.

From the **Wizards** menu in the ASDM menu bar, select the **High Availability and Scalability Wizard** option.

Ensure that you are on the primary (active) ASA.

Following are six steps for this wizard.

Step 1: Configuration Type

Select **Configure Active/Standby Failover** from the wizard screen 1 of 6.

Click **Next** to go to Step 2.

Step 2: Failover Peer Connectivity

Enter the IP address of the peer. This is the IP address that you configured for the secondary (standby) unit.

When you click **Next**, the following tests are performed to determine whether the ASA at the IP address you entered is a compatible failover peer for the ASA you are configuring:

- Connectivity test from this Cisco ASDM to the peer security appliance (secondary unit)
- Connectivity test from this security appliance (primary unit) to the peer security appliance (secondary unit)
- Hardware compatibility test
- Software version compatibility test
- Failover license compatibility test
- Routed or transparent firewall mode compatibility test
- Single or multiple context mode compatibility test

If all the tests are passed, you are ready for Step 3.

Step 3: LAN Link Configuration

Configure the failover interface to communicate between the primary and secondary ASAs.

You need to enter the following:

- Interface
- Logical name
- Active IP address
- Standby IP address
- Subnet mask
- Secret key (if encryption is being used)

Click **Next** to proceed to Step 4.

Step 4: State Link Configuration

In this step, you configure the stateful failover link. You have the options to do the following:

- Disable stateful failover
- Use the LAN link as the state link
- Configure a separate stateful failover interface

Click **Next** to go to Step 5.

 Please see page 110 for more details.

Step 5: Standby Address Configuration

Configure the standby IP address for each interface that has an active IP address. The active IP addresses are displayed, and the standby IP address must be on the same Layer 3 subnet and reachable from the active IP address.

By default, every interface is monitored for failure. If you do not want to monitor an interface, deselect the Monitored check box at the side of the interface.

Click **Next** to go to Step 6.

Step 6: Summary

The final step provides a summary of the configuration that you have just entered. You have the option at this point to review what you are about to do and if necessary go back into the wizard to amend any step.

When you are satisfied with your configuration, click the **Finish** button to complete the wizard and apply the configuration to the primary ASA.

The Waiting for Config Sync window displays. This window displays while the configuration from the primary ASA is transferred to the secondary ASA.

When this has completed, the failover configuration has been applied to both the primary and secondary ASA.

Step 4: Verify That Cisco ASDM Configured the Secondary Security Appliance with the LAN-Based Failover Command Set

After active/standby failover is configured on the primary unit, the configuration of the primary unit should have transferred over to the secondary unit. It is advisable to log on to the ASDM on the secondary unit and confirm that the secondary ASA has been configured for failover and contains the LAN-based failover command set.

 Please see page 110 for more details.

Step 5: Save the Configuration of the Secondary Security Appliance to Flash Memory

The fifth and final step is to save the configuration on both ASAs to flash memory.

A common mistake is to save the configuration to flash memory on the primary ASA and forget about the secondary ASA. When the secondary ASA is powered off, it loses its configuration unless the configuration is saved to flash.

Active/Active Failover Configuration

Now look at how to configure active/active failover on a pair of ASAs using the ASDM.

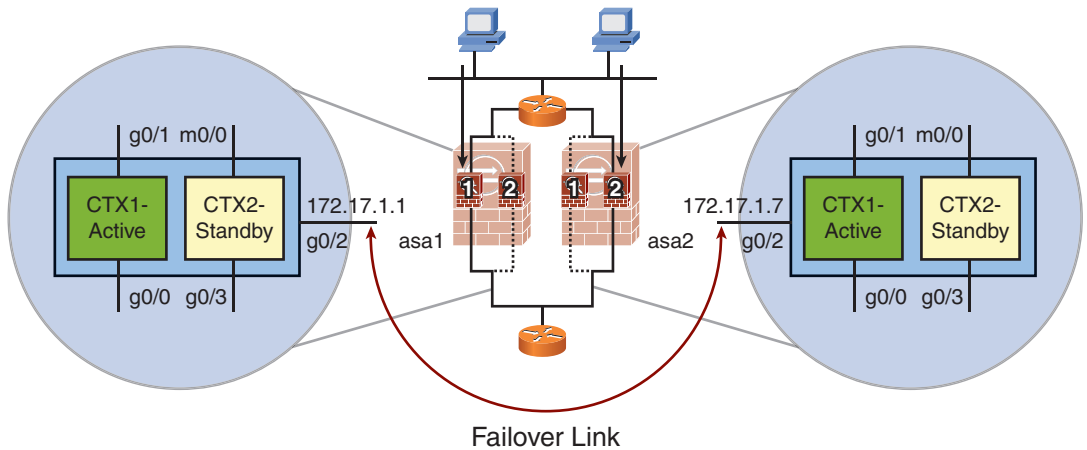
With active/standby failover, one ASA is active, and the other ASA is redundant, waiting to take over the role of the active ASA if a failure occurs. With active/active failover, the ASA firewalls must be configured in multiple context mode so that both devices can pass traffic while at the same time serving as a backup for the other peer ASA.

Active/active configuration leverages the virtual context feature on the ASA. Each ASA is partitioned into two contexts: CTX1 and CTX2. Under normal conditions, there is one active context and one standby context per ASA. The active context on one ASA has a standby context on the second ASA and vice versa.

Figure 71 shows an active/active failover.

 Please see page 110 for more details.

FIGURE 71
Active/Active Failover Network



When one context or ASA fails, the other ASA takes over the active role for either, or both, contexts.

Following are eight steps to configure active/standby failover:

Step 1: Cable the interfaces on both ASAs.

Step 2: Ensure that both ASAs are in multiple context mode.

Step 3: Configure contexts and allocate interfaces to contexts.

Step 4: Enable and assign IP addresses to each interface allocated to a context.

Step 5: Prepare both security appliances for configuration via ASDM.

Step 6: Use the ASDM High Availability and Scalability Wizard to configure the ASA for failover.

Step 7: Verify that ASDM configured the secondary ASA with the LAN-based failover command set.

Step 8: Save the configuration of the secondary ASA to flash.

 Please see page 110 for more details.

Step 1: Cable the Interfaces on Both ASAs

The first step is to cable the interfaces on both of the ASAs so that the corresponding interfaces are on common networks.

A LAN-based failover connection is required between the two ASAs. If you plan to use stateful failover, an interface on the ASA must be dedicated to this function, unless you configure stateful failover to share the same interface as the LAN-based failover connection.

Step 2: Ensure That Both ASAs Are in Multiple Context Mode

For active/active failover to work, both ASAs must be in multiple context mode.

Step 3: Configure Contexts and Allocate Interfaces to Contexts

Ensure that the contexts are created and that the interfaces are allocated into the corresponding contexts.

Step 4: Enable and Assign IP Addresses to Each Interface Allocated to a Context

Both ASAs require an IP address be assigned on the inside interface that can be accessed via ASDM.

Step 5: Prepare Both Security Appliances for Configuration via ASDM

Prepare both ASAs for ASDM configuration. Section 2 of this Quick Reference guide covered how to configure the ASA so that you can access it using ASDM.

Both ASAs require an IP address be assigned on the inside interface that can be accessed via ASDM.

 Please see page 110 for more details.

Step 6: Use the ASDM High Availability and Scalability Wizard to Configure the ASA for Failover

Configure active/active failover using the High Availability and Scalability Wizard on the ASDM.

From the **Wizards** menu in the ASDM menu bar, select the **High Availability and Scalability Wizard** option.

Ensure that you are on the system context.

Following are seven steps for this wizard.

Step 1: Configuration Type

Select **Configure Active/Active Failover** from the wizard screen 1 of 6.

If you are not in multiple context mode, the ASA prompts you to change the context mode and warns you of the consequences.

Click **Next** to go to Step 2.

Step 2: Failover Peer Connectivity

Enter the IP address of the peer. This is the IP address that you configured for the second ASA that will act in the active/active failover pair. This does not have to be the failover link address, but it does have to be the IP address that has ASDM access enabled on it.

When you click **Next**, the following tests are performed to determine whether the ASA at the IP address you entered is a compatible failover peer for the ASA you are configuring:

- Connectivity test from this Cisco ASDM to the peer security appliance (secondary unit)
- Connectivity test from this security appliance (primary unit) to the peer security appliance (secondary unit)
- Hardware compatibility test

 Please see page 110 for more details.

- Software version compatibility test
- Failover license compatibility test
- Routed or transparent firewall mode compatibility test
- Single or multiple context mode compatibility test

If all the tests are passed, you are taken to Step 3.

Step 3: Security Context Configuration

At Step 3, you assign security contexts to failover groups. The page displays the security contexts currently configured on the ASA along with the failover group each context belongs to. By default, both contexts are assigned to group 1.

Click **Next** to go to Step 4.

Step 4: LAN Link Configuration

Now configure the failover interface that communicates between this ASA and the failover peer.

You need to enter the following:

- Interface
- Logical name
- Active IP address
- Standby IP address
- Subnet mask
- Secret key (if encryption is being used)

 Please see page 110 for more details.

Click **Next** to go to Step 5.

Step 5: State Link Configuration

In this step, you configure the stateful failover link. You have the options to do the following:

- Disable stateful failover.
- Use the LAN link as the state link.
- Configure a separate stateful failover interface.

Click **Next** to go to Step 6.

Step 6: Standby Address Configuration

This step enables you to configure the standby IP address for each interface that has an active IP address. The active IP addresses display, and the standby IP address must be on the same Layer 3 subnet and reachable from the active IP address.

By default, every interface is monitored for failure. If you do not want to monitor an interface, deselect the Monitored check box at the side of the interface.

From this screen, you can determine which contexts are in which failover groups and which interfaces are allocated to each context.

Click **Next** to go to Step 7.

Step 7: Summary

The final step provides a summary of the configuration that you have just entered. You have the option at this point to review what you are about to do, and if necessary you can go back into the wizard to amend any step.

When you are happy with your configuration, click the **Finish** button to complete the wizard and apply the configuration to the ASA you are configuring.

 Please see page 110 for more details.

The Waiting for Config Sync window now displays. This window displays while the configuration is transferred to the active failover peer ASA. When this has completed, the failover configuration has been applied to both of the ASAs operating as failover peers.

Step 7: Verify That ASDM Configured the Secondary ASA with the LAN-Based Failover Command Set

After failover is configured on the primary unit, the configuration of the primary unit should have transferred over to the secondary unit. It is advisable to log on to both failover peers' ASDM and verify the LAN-based failover command set.

Step 8: Save the Configuration of the Secondary ASA to Flash

The eighth and final step is to save the configuration on both ASAs to flash memory.

A common mistake is to save the configuration to flash memory on the primary ASA and forget about the failover peer. You need to ensure that the configuration is saved to flash memory on both of the failover peer ASAs.

ASA Redundant Interfaces

In addition to device-level failover, you can configure a redundant interface. Redundant interfaces can be used with device-based failover or alone to increase the reliability of the ASA.

A redundant interface is a logical interface consisting of two physical interfaces. One physical interface serves as the active interface whereas the other serves as the standby. When the active interface fails, the standby interface becomes active and starts passing traffic. It does not load share across both interfaces at the same time. A redundant interface is considered in failure state only when both of the underlying physical interfaces fail.

 Please see page 110 for more details.

When you configure redundant interfaces. The entire ASA configuration refers to the logical redundant interface rather than the physical interfaces.

To configure a redundant interface, navigate to the **Device Setup > Interfaces** screen, click the **Add** button, and then choose **Redundant Interface**.

Summary

This section covered failover on the ASA. Failover is a mechanism to protect your network from failure if the ASA should fail for any reason. You looked at the two types of failover available on the ASA: active/standby and active/active.

This brings you to the end of this Quick Reference on the Cisco ASA Fundamentals.

 Please see page 110 for more details.

CCNP Security Firewall 642-617 Quick Reference

Andrew Mason

Technical Editor: **Max Leitch**

Published by:

Cisco Press

800 East 96th Street

Indianapolis, IN 46240 USA

First Printing January 2011

ISBN-10: 0-13-256643-5

ISBN-13: 978-0-13-256643-8

Warning and Disclaimer

This book is designed to provide information about the CCNP Security Firewall exam. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc

Trademark Acknowledgments

All terms mentioned in this ebook that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc. cannot attest to the accuracy of this information. Use of a term in this ebook should not be regarded as affecting the validity of any trademark or service mark.

Feedback Information

At Cisco Press, our goal is to create in-depth technical ebooks of the highest quality and value. Each ebook is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members of the professional technical community.

Reader feedback is a natural continuation of this process. If you have any comments on how we could improve the quality of this ebook, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please be sure to include the ebook title and ISBN in your message.

We greatly appreciate your assistance.

Corporate and Government Sales

The publisher offers excellent discounts on this ebook when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact: **U.S. Corporate and Government Sales** 1-800-382-3419 corpsales@pearsontechgroup.com.

For sales outside the United States please contact: **International Sales** international@pearsoned.com

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.**