SNPA

Securing Networks with PIX and ASA

Volume 1

Version 4.0

Student Guide

CLS Production Services: 07.11.05

Table of Contents

Volume 1

Table of Contents

Volume 2

Table of Contents

Volume 3

Course Introduction

Overview

Securing Networks with PIX and ASA (SNPA) v4.0 provides the learner with the skills necessary to configure, maintain, and operate PIX security appliances and ASA security appliances.

Learner Skills and Knowledge

This subtopic lists the skills and knowledge that learners must possess to benefit fully from the course. The subtopic also includes recommended Cisco learning offerings that learners should complete in order to benefit fully from this course.

Learner Skills and Knowledge

Cisco.com

- **Cisco CCNA certification or the equivalent knowledge**
- **Basic knowledge of the Windows operating system**
- **Familiarity with networking and security terms and concepts**

SNPA v4.0—3

Course Goal and Objectives

This topic describes the course goal and objectives.
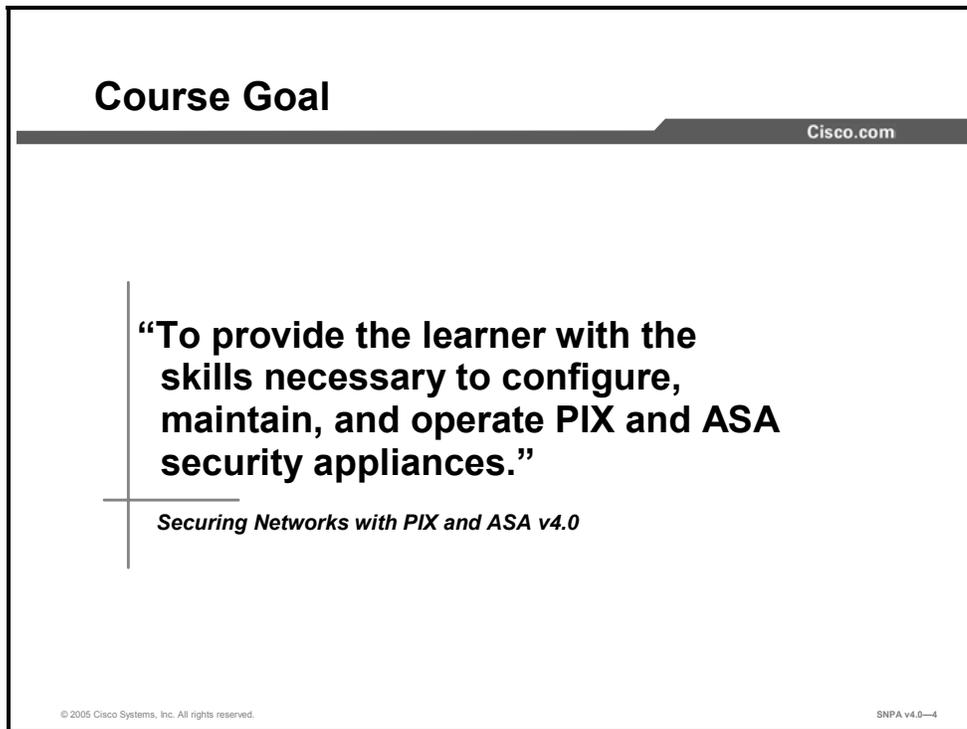
Course Goal

"To provide the learner with the
skills necessary to configure,
maintain, and operate PIX and ASA
security appliances."

Securing Networks with PIX and ASA v4.0

SNPA v4.0—4

Upon completing this course, you will be able to meet these objectives:

■ Describe firewall technology and security appliance features

■ Describe security appliance models, option cards, and licenses

■ Configure security appliances to statically and dynamically translate IP addresses

■ Configure security appliances to control inbound and outbound traffic

■ Configure object groups to simplify ACL configuration

■ Explain the routing functionality of security appliances

■ Configure a modular policy in security appliances

■ Configure advanced protocol handling on security appliances

■ Configure AAA on security appliances

■ Configure active/standby, active/active, and stateful failover on security appliances

■ Load and initialize IPS software on the AIP-SSM module

■ Configure security appliances for site-to-site VPNs, remote access VPNs, and WebVPNs

■ Configure client-to–security appliance VPNs

■ Configure security appliance management

■ Install the Cisco Adaptive Security Device Manager and use it to configure and monitor a security appliance

Course Flow

This topic presents the suggested flow of the course materials.

Course Flow

Cisco.com

Day 1	Day 2	Day 3	Day 4	Day 5
A M Course Introduction Lesson 1: Cisco Security Appliance Technology and Features Lesson 2: Cisco PIX Security Appliance and ASA Adaptive Security Appliance Families	Lesson 5: Access Control Lists and Content Filtering Lesson 6: Object Grouping	Lesson 9: Modular Policy Framework Lesson 10: Advanced Protocol Handling	Lesson 13: Configuring ASA for WebVPN Lesson 14: Configuring Transparent Firewall	Lesson 17: Cisco Security Appliance Device Manager Lesson 18: AIP-SSM—Getting Started
Lunch				
P M Lesson 3: Getting Started with Cisco Security Appliances Lesson 4: Translations and Connections	Lesson 7: Authentication, Authorization, and Accounting Lesson 8: Switching and Routing	Lesson 11: VPN Configuration Lesson 12: Configuring Security Appliance Remote Access Using Cisco Easy VPN	Lesson 15: Configuring Security Contexts Lesson 16: Failover	Lesson 19: Managing Security Appliances

SNPA v4.0—5

The schedule reflects the recommended structure for this course. This structure allows enough time for the instructor to present the course information and for you to work through the lab activities. The exact timing of the subject materials and labs depends on the pace of your specific class.

Additional References

This topic presents the Cisco icons and symbols used in this course, as well as information on where to find additional technical references.

Graphic Symbols

Cisco.com

IOS Router   Security Appliance   VPN 3000   IPS Sensor   Catalyst 6500 w/ IPS Module   IOS Firewall

Network Access Server   Policy Manager   CA Server   PC   Laptop   Server Web, FTP, etc.

Hub   Modem   Ethernet Link   VPN Tunnel   Network Cloud

SNPA v4.0—6
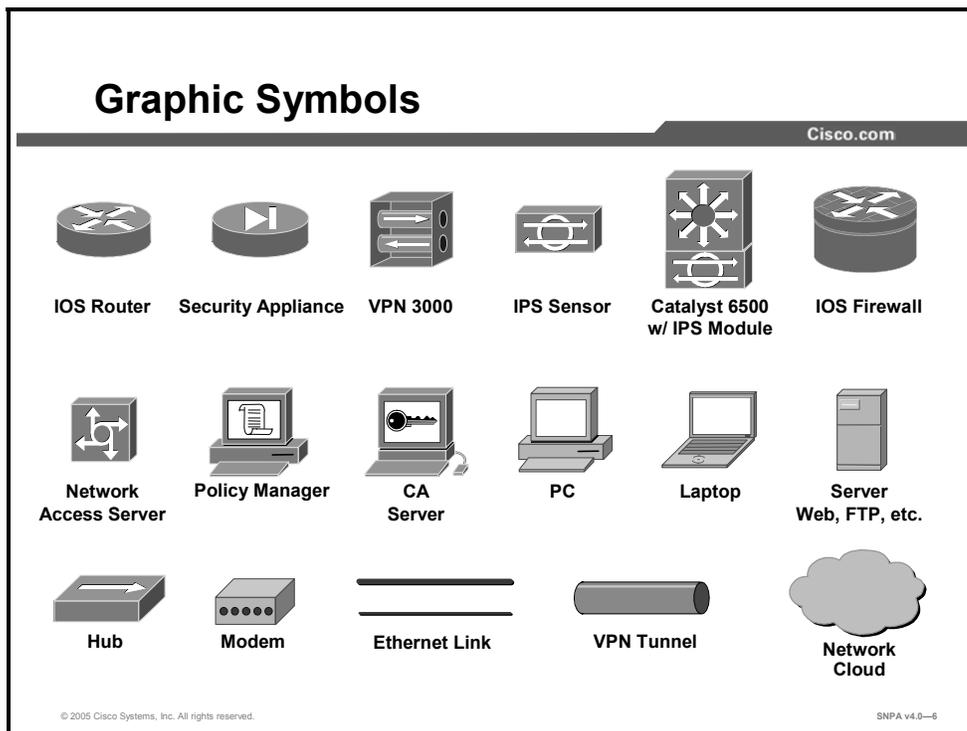
Cisco Glossary of Terms

For additional information on Cisco terminology, refer to the Cisco Internetworking Terms and Acronyms glossary of terms at
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm.

Lesson 1

Cisco Security Appliance Technology and Features

Overview

This lesson describes the three technologies that firewall operation is based on: packet filtering, proxy server, and stateful packet filtering. The lesson continues with a discussion of the features of Cisco security appliances.

Objectives

Upon completing this lesson, you will be able to describe the general functionality provided by firewalls and security appliances. This includes being able to meet these objectives:

- Explain the functions of the three types of firewalls used to secure today's computer networks

- Discuss the technology and features of Cisco security appliances

Firewalls

This topic explains firewalls.

What Is a Firewall?

DMZ Network

Internet

Outside Network

Inside Network

A firewall is a system or group of systems that manages access between two or more networks.

SNPA v4.0—1-3
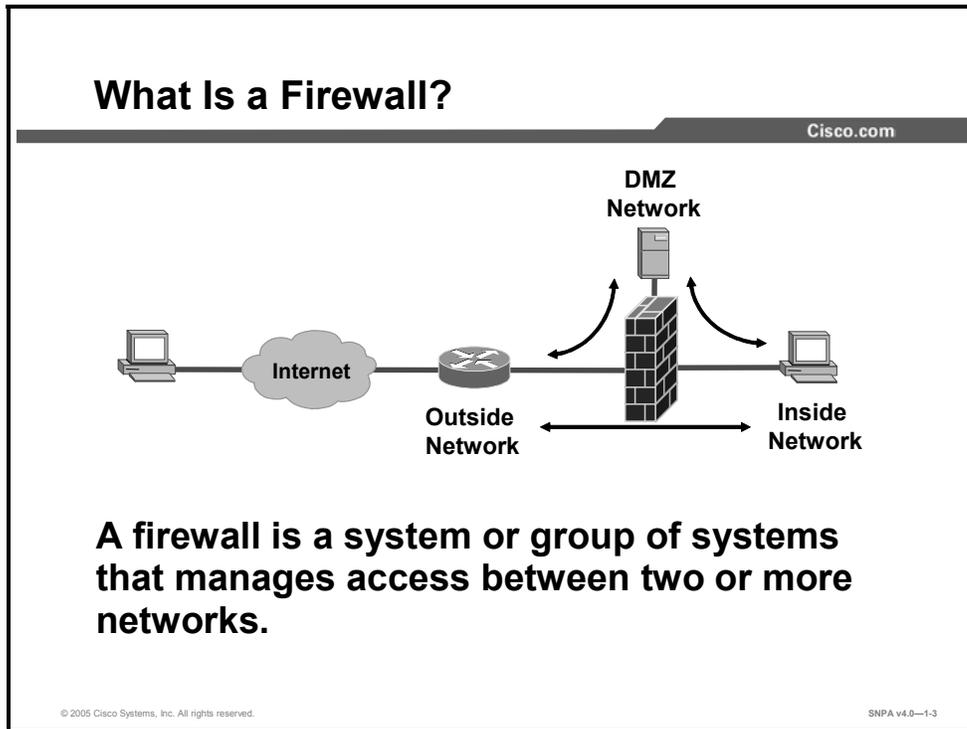
By conventional definition, a firewall is a partition made of fireproof material designed to prevent the spread of fire from one part of a building to another. It can also be used to isolate one compartment from another.

When applying the term to a computer network, a firewall is a system or group of systems that manages access between two or more networks.

Firewall Technologies

Firewall operations are based on one of three technologies:

- **Packet filtering**
- **Proxy server**
- **Stateful packet filtering**

Firewall operations are based on one of these three technologies.

■ Packet filtering: Limits information that is allowed into a network based on static packet header information

■ Proxy server: Requests connections on behalf of the client on the inside of the firewall and the Internet

■ Stateful packet filtering: Combines the best of packet filtering and proxy server technologies

Packet Filtering

DMZ:
Server B

Host A

Data | A | B

Inside:
Server C

Internet

Data | A | C

AB-Yes
AC-No
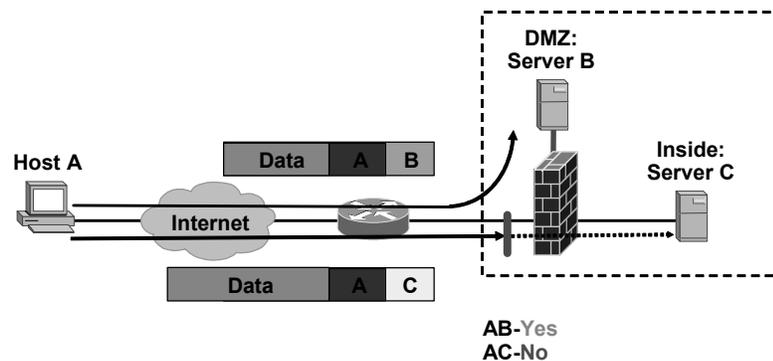
**Limits information that is allowed into a network
based on the destination and source address**

SNPA v4.0—1-5

A firewall can use packet filtering to limit information that enters a network and information moving from one segment of a network to another. Packet filtering uses access control lists (ACLs), which allow a firewall to accept or deny access based on packet types and other variables.

This method is effective when a protected network receives a packet from an unprotected network. Any packet that is sent to the protected network and does not fit the criteria defined by the ACLs is dropped.

Problems with packet filtering are as follows:

- Arbitrary packets can be sent that fit the ACL criteria and therefore pass through the filter.

- Packets can pass through the filter by being fragmented.

- Complex ACLs are difficult to implement and maintain correctly.

- Some services cannot be filtered.

Proxy Server

Proxy Server

Internet

Outside Network

Inside Network
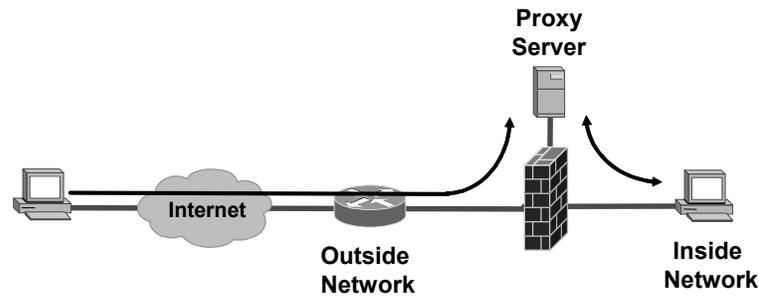
Requests connections on behalf of a client that is inside the firewall and the Internet

SNPA v4.0—1-6

A proxy server is a firewall device that examines packets at higher layers of the Open Systems Interconnection (OSI) model. This device hides valuable data by requiring users to communicate with a secure system by means of a proxy. Users gain access to the network by going through a process that establishes session state, user authentication, and authorized policy. This means that users connect to outside services via application programs (proxies) that are running on the gateway that is connected to the outside unprotected zone.

Problems with the proxy server are as follows:

- The proxy server creates a single point of failure, which means that if the entrance to the network is compromised, then the entire network is compromised.

- Adding new services to the firewall is difficult.

- The proxy server performs more slowly under stress.

Stateful Packet Filtering

DMZ:
Server B

Host A | Data | HTTP | A | B

Internet

Inside:
Server C

Limits information that is allowed into a network based not only on the destination and source addresses, but also on the packets state table content

State Table

Source address	192.168.0.20	10.0.0.11
Destination address	172.16.0.50	172.16.0.50
Source port	1026	1026
Destination port	80	80
Initial sequence #	49769	49091
Ack		
Flag	Syn	Syn
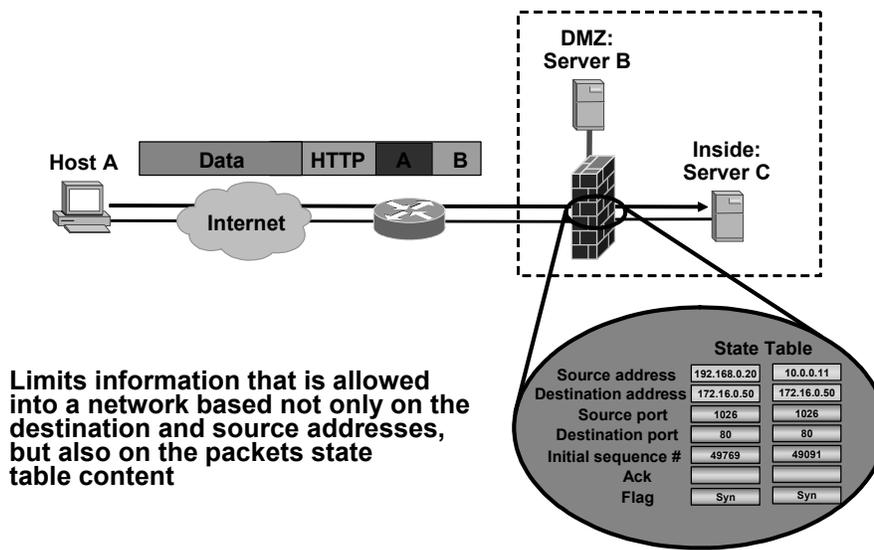
SNPA v4.0—1-7

Stateful packet filtering is the method that is used by the Cisco security appliances. This technology maintains complete session state. Each time a TCP or User Datagram Protocol (UDP) connection is established for inbound or outbound connections, the information is logged in a stateful session flow table.

The stateful session flow table, also known as the state table, contains the source and destination addresses, port numbers, TCP sequencing information, and additional flags for each TCP or UDP connection that is associated with that particular session. This information creates a connection object, and consequently, all inbound and outbound packets are compared against session flows in the stateful session flow table. Data is permitted through the firewall only if an appropriate connection exists to validate its passage.

This method is effective for three reasons.

■   It works both on packets and on connections.

■   It operates at a higher performance level than packet filtering or using a proxy server.

■   It records data in a table for every connection and connectionless transaction. This table serves as a reference point for determining if packets belong to an existing connection or are from an unauthorized source.

Security Appliance Overview

This topic discusses the basic concepts of security appliances.

Security Appliances: What Are They?

Cisco.com

Cisco security appliances deliver enterprise-class security for small-to-medium-sized business and enterprise networks in a modular, purpose-built appliance. Some features of Cisco security appliances are:

- **Proprietary operating system**
- **Stateful packet inspection**
- **User-based authentication**
- **Protocol and application inspection**
- **Modular policy**
- **Virtual private networking**
- **Security contexts (virtual firewalls)**
- **Stateful failover capabilities**
- **Transparent firewalls**
- **Web-based management solutions**

© 2005 Cisco Systems, Inc. All rights reserved.

SNPA v4.0—1-9

The Cisco PIX 500 Series Security Appliances and the Cisco ASA 5500 Series Adaptive Security Appliances (Cisco ASA security appliances) are a key element in the overall Cisco end-to-end security solution. The market-leading Cisco security appliances provide enterprise-class, integrated network security services—including stateful inspection firewalling, protocol and application inspection, virtual private networks (VPNs), in-line intrusion prevention, and rich multimedia and voice security—in cost-effective, easy-to-deploy solutions. Ranging from compact "plug-and-play" desktop firewalls for small offices to carrier-class gigabit firewalls for the most demanding enterprise and service-provider environments, Cisco security appliances provide robust security, performance, and reliability for network environments of all sizes.

Some features of the Cisco PIX security appliances and ASA security appliances are as follows:

- Security, performance, and reliability in purpose-built security appliances

- State-of-the-art stateful packet inspection

- 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 next-generation security policy framework

- Robust VPN for secure site-to-site and remote access connections

- Multiple security contexts (virtual firewalls) within a single appliance

- Stateful failover capabilities that ensure resilient network protection

- Transparent deployment of security appliances into existing network environments without requiring readdressing of the network

- Integrated intrusion prevention to guard against popular Internet threats, such as denial of service (DoS) attacks

- Robust remote manageability using Cisco Adaptive Security Device Manager (ASDM), Telnet, Secure Socket Layer (SSL), Secure Shell Protocol (SSH), Simple Network Management Protocol (SNMP), and syslog

Proprietary Operating System

Eliminates the risks associated with general-purpose operating systems

SNPA v4.0—1-10

The Cisco security appliance operating system is a non-UNIX, non-Windows NT, Cisco IOS software-like operating system. Use of the Cisco security appliance operating system eliminates the risks associated with general-purpose operating systems. It enables the PIX security appliances and ASA security appliances to deliver outstanding performance with up to 500,000 simultaneous connections.

Stateful Packet Inspection

- **The stateful packet inspection algorithm provides stateful connection security:**
  - **It tracks source and destination ports and addresses, TCP sequence numbers, and additional TCP flags.**
  - **It randomizes the initial TCP sequence number of each new connection.**
- **By default, the stateful packet inspection algorithm allows connections originating from hosts on inside (higher security level) interfaces.**
- **By default, the stateful packet inspection algorithm drops connection attempts originating from hosts on outside (lower security level) interfaces.**
- **The stateful packet inspection algorithm supports authentication, authorization, and accounting.**

SNPA v4.0—1-11

The heart of the security appliance is the stateful packet inspection algorithm. The stateful packet inspection algorithm maintains the secure perimeters between the networks that are controlled by the security appliance. The connection-oriented stateful packet inspection algorithm design creates session flows based on source and destination addresses. It randomizes TCP sequence numbers, port numbers, and additional TCP flags before completion of the connection. This function is always in operation, monitoring return packets to ensure that they are valid, and allows one-way (inside to outside) connections without an explicit configuration for each internal system and application. Randomizing of the TCP sequence numbers minimizes the risk of a TCP sequence number attack. Because of the stateful packet inspection algorithm, the security appliance is less complex and more robust than a packet filtering-designed firewall.

Stateful packet filtering is a secure method of analyzing data packets that places extensive information about a data packet into a table. Each time a TCP connection is established for inbound or outbound connections through the security appliance, the information about the connection is logged in a stateful session flow table. For a session to be established, information about the connection must match information stored in the table. With this methodology, the stateful filters work on the connections and not the packets, making it a more stringent security method, with its sessions immune to hijacking.

Stateful packet filtering does the following:

- Obtains the session-identifying parameters, IP addresses, and ports for each TCP connection
- Logs the data in a stateful session flow table and creates a session object
- Compares the inbound and outbound packets against session flows in the connection table
- Allows data packets to flow through the security appliance only if an appropriate connection exists to validate their passage
- Temporarily sets up a connection object until the connection is terminated

Cut-Through Proxy Operation

1. The user makes a request to an ISP.

Internal or External User

2. The security appliance intercepts the connection.

3. At the application layer, the security appliance prompts the user for a username and password. It then authenticates the user against a RADIUS or TACACS+ server and checks the security policy.

3. Username and Password Required

Enter username for CCO at www.com

User Name: student

Password: 123@456

OK   Cancel

Cisco Secure

ISP

4. The security appliance initiates a connection from the security appliance to the destination ISP.

5. The security appliance directly connects the internal or external user to the ISP via the security appliance. Communication then takes place at a lower level of the OSI model.

SNPA v4.0—1-12

Cut-through proxy is a method of transparently verifying the identity of the users at the security appliance and permitting or denying access to any TCP- or UDP-based applications. This is also known as user-based authentication of inbound and outbound connections. Unlike a proxy server, which analyzes every packet at the application layer of the OSI model, the security appliance first challenges a user at the application layer. After the user is authenticated and the policy is checked, the security appliance shifts the session flow to a lower layer of the OSI model for dramatically faster performance. This allows security policies to be enforced on a per-user-identification basis.

Connections must be authenticated with a user identification and password before they can be established. The user identification and password is entered via an initial Hypertext Transfer Protocol (HTTP), HTTP secure (HTTPS), Telnet, or File Transfer Protocol (FTP) connection. This method eliminates the price performance impact that UNIX system-based firewalls impose in similar configurations and allows a finer level of administrative control over connections. The cut-through proxy method of the security appliance also leverages the authentication and authorization services of the Cisco Secure Access Control Server (Cisco Secure ACS). The security appliance is interoperable and scalable with IPSec, which includes an umbrella of security and authentication protocols, such as Internet Key Exchange (IKE) and public key infrastructure (PKI). The security appliance offers an IPSec-based VPN. Remote clients can securely access corporate networks through their ISPs.

Application-Aware Inspection

FTP Server

Client

Data Port 20   Control Port 21

Control Port 2008   Data Port 2010

Data - Port 2010

Port 2010 OK

Data
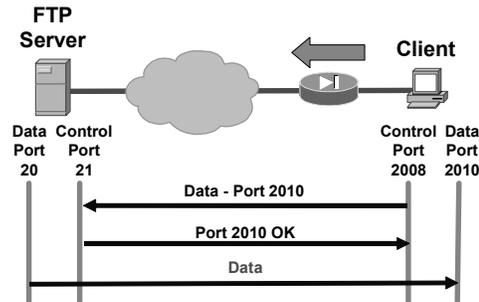
- **Protocols such as FTP, HTTP, H.323, and SQL*Net need to negotiate connections to dynamically assigned source or destination ports through the firewall.**
- **The security appliance inspects packets above the network layer.**
- **The security appliance securely opens and closes negotiated ports for legitimate client-server connections through the firewall.**

SNPA v4.0—1-13

Today many corporations use the Internet for business transactions. For the corporations to keep their internal networks secure from potential threats from the Internet, they can implement firewalls on their internal network. Even though these firewalls help protect a corporation's internal networks from external threats, firewalls have caused problems as well. For example, some of the protocols and applications that the corporations use to communicate are not allowed through the firewalls. Specifically, protocols need to negotiate FTP, HTTP, H.323, and SQL*Net connections to dynamically assigned source ports, destination ports, or IP addresses, through the firewall.

A good firewall has to inspect packets above the network layer and do the following as required by the protocol or application:

- Securely open and close negotiated ports or IP addresses for legitimate client-server connections through the firewall

- Use Network Address Translation (NAT)-relevant instances of an IP address inside a packet

- Use port address translation (PAT)-relevant instances of ports inside a packet

- Inspect packets for signs of malicious application misuse

You can configure the security appliance to allow the required protocols or applications through the security appliance. This enables a corporation's internal networks to remain secure while still continuing day-to-day business over the Internet.

Modular Policy

Cisco.com
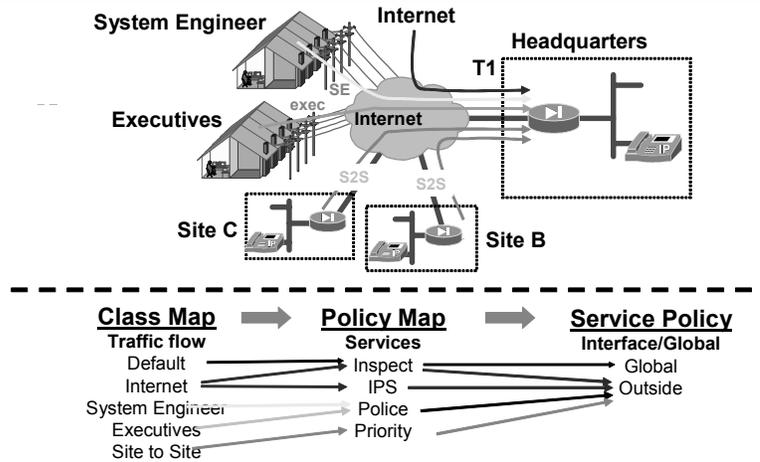
Construction of flow-based policies:
• **Identify specific flows.**
• **Apply services to that flow.**

SNPA v4.0—1-14

Cisco PIX and ASA Security Appliance Software v7.0 introduces a highly flexible and extensible next-generation security policy framework. It enables the construction of flow-based policies that identify specific flows based on administrator-defined conditions, then apply a set of services to that flow (such as inspection policies, VPN policies, quality of service [QoS] policies, and more). In the figure, four traffic flows are identified: Internet traffic, system engineer traffic, executive VPN traffic, and site-to-site voice traffic. Service policies were applied to each of the flows—for example, in the site-to-site traffic flow, voice is given priority; in the VPN flows, each group's traffic throughput is policed; and Internet traffic undergoes application inspection and is routed through an Intrusion Prevention System (IPS) module. This provides significantly improved granular control over traffic flows and the services performed on them. This new framework also enables inspection engines to have flow-specific settings.

Virtual Private Network

Site to Site

Internet

**IPSec VPN
SSL VPN**

Remote Access
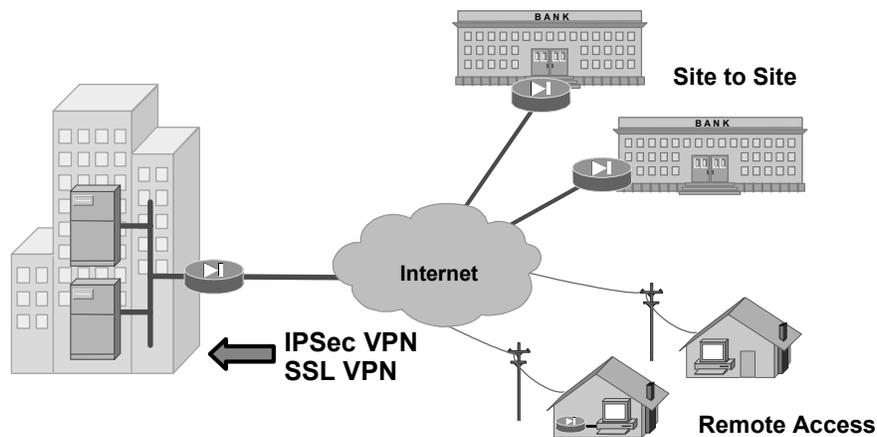
SNPA v4.0—1-15

A VPN is a service that offers secure, reliable connectivity over a shared public network infrastructure such as the Internet. Because the infrastructure is shared, connectivity can be provided at a cost that is lower than that of existing dedicated private networks. The security appliance enables IPSec VPNs for both site-to-site and remote access networks. WebVPN complements IPSec-based remote access by allowing secure remote access to corporate network resources without the use of VPN client software (supported only on ASA security appliances).

Security Context (Virtual Firewall)

Cisco.com

Four Physical Firewalls

**One Physical Firewall
Four Virtual Firewalls**

Internet

Internet
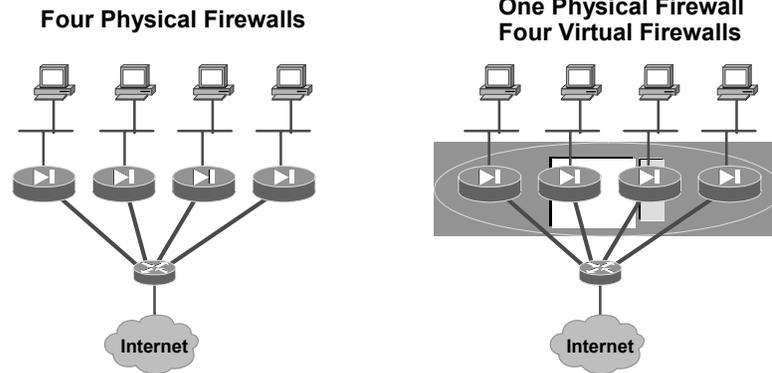
- **Ability to create multiple security contexts (virtual firewalls) within a single security appliance**

SNPA v4.0—1-16

Cisco PIX and ASA Security Appliance Software v7.0 introduces the ability to create multiple security contexts (virtual firewalls) within a single appliance, with each context having its own set of security policies, logical interfaces, and administrative domain. In the figure, the security appliance on the right is logically divided into four virtual firewalls. This provides businesses with a convenient way to consolidate multiple firewalls into a single physical appliance, yet to retain the ability to manage each of these virtual instances separately. These capabilities are only available on Cisco PIX 500 Series security appliances with either an unrestricted license (UR license) or a failover license (FO license) and Cisco ASA 5520 and 5540 Adaptive Security Appliances. This is a licensed feature, with multiple tiers of supported security contexts (2, 5, 10, 20, and 50).

Failover Capabilities: Active/Standby, Active/Active, and Stateful Failover

Cisco.com

Failover: Active/Standby

Failover: Active/Active

Contexts

Primary: **Failed Firewall**

Secondary: **Active Firewall**

Primary: **Failed/Standby**

Secondary: **Active/Active**

Internet

Internet
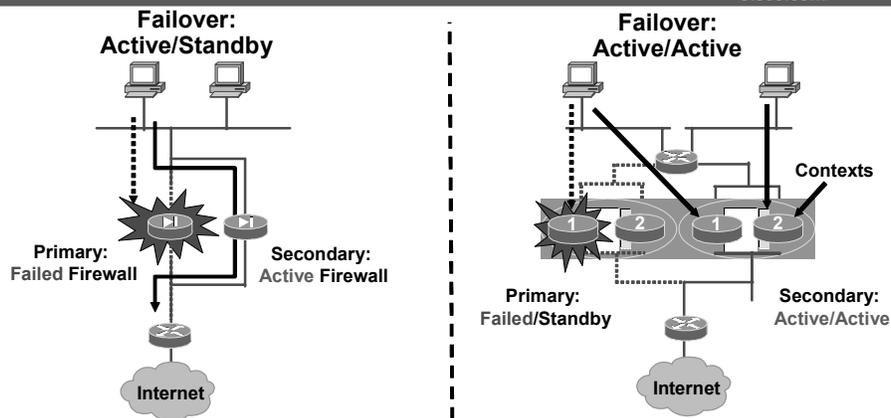
- **Failover protects the network should the primary go offline.**
  - **Active/standby—Only one unit can be actively processing traffic; the other is hot standby.**
  - **Active/Active—Both units can process traffic and serve as backup units.**
- **Stateful failover maintains operating state during failover.**

SNPA v4.0—1-17

Failover provides a mechanism for the security appliance to be redundant by allowing two identical security appliances, hardware and software, to serve the same functionality. The active security appliance performs normal security functions while the standby security appliance monitors, ready to take control should the active security appliance fail. Under the active/standby failover model, only one security appliance actively processes user traffic while the other unit acts as a hot standby, prepared to take over if the active unit fails. In the active/standby example in the figure, the primary security appliance has failed and the secondary security appliance becomes active. After the failure, all traffic flows through the secondary security appliance.

Cisco PIX and ASA Security Appliance Software v7.0 supports a two-node active/active failover configuration with two failover groups. The active/active failover feature requires security contexts. The active/active example in the figure displays a two-security-appliance failover cluster. Each security appliance has two contexts. Under normal conditions in each security appliance, one context is active and the other is standby. One context actively processes firewall traffic while the other context serves as a backup for the other security appliance. As in the active/standby example, when one of the security appliances fails in an active/active failover, the other security appliance will have both contexts active and will process 100 percent of the traffic.

In both of these scenarios, the security appliance can be configured for stateful failover so that active connections remain when failover occurs. The stateful feature passes per-connection stateful information to the standby unit. After a failover occurs, the same connection information must be available at the new unit.

Transparent Firewall

192.168.1.5

192.168.1.2

Internet
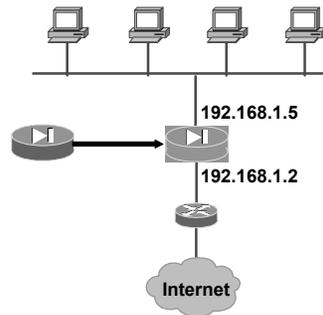
- **Has the ability to deploy a security appliance in a secure bridging mode**
- **Provides rich Layers 2 through 7 security services as a Layer 2 device**

Cisco PIX and ASA Security Appliance Software v7.0 debuts the ability to deploy a security appliance in a secure bridging mode as a Layer 2 device to provide rich Layers 2 through 7 security services for the protected network. This enables businesses to deploy security appliances into existing network environments without requiring readdressing of the network. Although the security appliance can be completely invisible to devices on both sides of a protected network, administrators can manage it via an exposed IP address (which can be hosted on a separate interface). Administrators also have the ability to specify Ethertype-based ACLs for access control over Layer 2 devices and protocols.

Web-Based Management Solutions

Adaptive Security Device Manager

SNPA v4.0—1-19

The ASDM browser-based configuration tool is designed to help you set up, configure, and monitor your security appliances graphically, without requiring extensive knowledge of the command-line interface (CLI) of the security appliance.

ASDM monitors and configures a *single* security appliance. You can use ASDM to create a new configuration and to monitor and maintain current security appliances. You can point your browser to more than one security appliance and administer several security appliances from a single workstation.

Summary

This topic summarizes what you learned in this lesson.

Summary

- **There are three firewall technologies: packet filtering, proxy server, and stateful packet filtering.**
- **Features of the Cisco PIX Firewall Security Appliances and ASA Security Appliances features include the following: proprietary operating system, stateful packet inspection, cut-through proxy, stateful failover, modular policy, VPNs, transparent firewall, security contexts, web-based management, and stateful packet filtering.**

SNPA v4.0—1-20

Cisco PIX Security Appliance and ASA Adaptive Security Appliance Families

Overview

The purpose of this lesson is to introduce the Cisco PIX 500 Series Security Appliances, the Cisco ASA 5500 Series Adaptive Security Appliances, and the Cisco Firewall Services Module.

Objectives

Upon completing this lesson, you will be able to choose the most appropriate firewall appliance and licensing for a given scenario. This includes being able to meet these objectives:

- Identify the Cisco PIX Security Appliance and ASA Adaptive Security Appliance models
- Describe the key features of the each security appliance
- Identify the controls, connectors, and LEDs of each security appliance
- Identify the interfaces of each security appliance
- Identify the security appliance expansion cards
- Explain the security appliance licensing options
- Describe the key features of the Cisco Firewall Services Module

Models and Features of Cisco Security Appliances

This topic describes the Cisco PIX 500 Series Security Appliance family and the Cisco ASA 5500 Adaptive Security Appliance family.
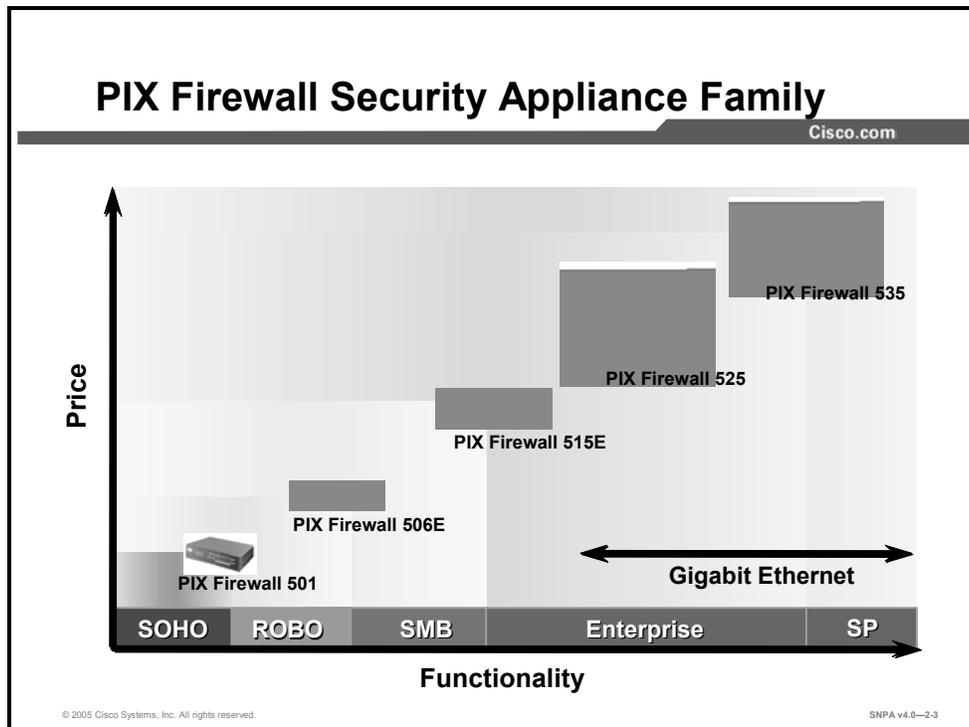
The Cisco PIX 500 Security Appliance series and Cisco ASA 5500 Series Adaptive Security Appliance scale to meet a range of requirements and network sizes. The PIX 500 Series Security Appliance family currently consists of five models: the PIX 501, 506E, 515E, 525, and 535 Security Appliances. The PIX 501 Security Appliance has an integrated 10/100BASE-T port (100BASE-T option is available in Cisco PIX Security Appliance Software v6.3) and an integrated four-port 10/100 switch. The PIX 506E Security Appliance has dual integrated 10/100BASE-T ports (100BASE-T option is available in Cisco PIX Security Appliance Software v6.3 for 506E only). The PIX 515E Security Appliance supports single-port or four-port 10/100 Ethernet cards in addition to two integrated 10/100BASE-T ports. The PIX 525 Security Appliance supports single-port or four-port 10/100 Fast Ethernet and Gigabit Ethernet in addition to two integrated 10/100BASE-T ports. The PIX 535 Security Appliance supports Fast Ethernet and Gigabit Ethernet in addition to two integrated 10/100BASE-T ports. The PIX 515E, 525, and 535 Security Appliance models come with an integrated virtual private network (VPN) Accelerator Plus card (VAC+).

The PIX Security Appliance is secure right out of the box. After a few installation procedures and an initial configuration of six general commands, your PIX Security Appliance is operational and protecting your network.

Note	Cisco PIX and ASA Security Appliance Software v7.0 does not support PIX 501, 506, or 506E Security Appliances.

ASA Adaptive Security Appliance Family
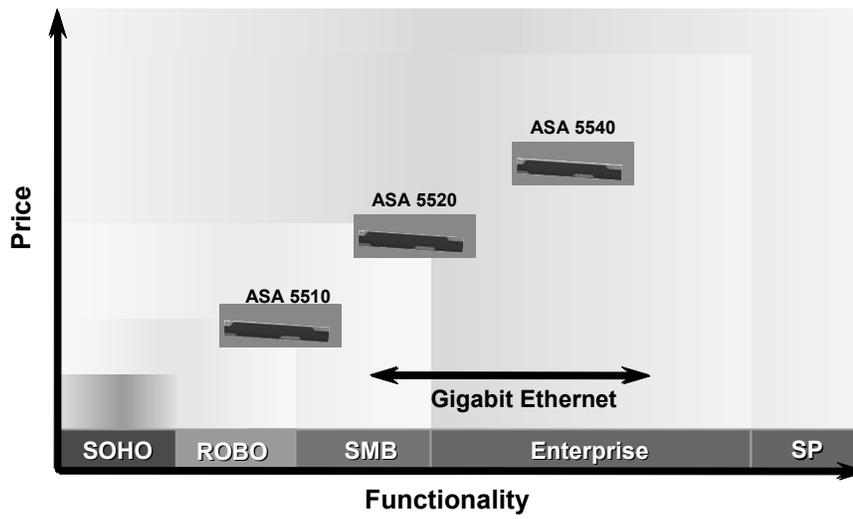
ASA 5540

ASA 5520

ASA 5510

Price

Gigabit Ethernet

| SOHO | ROBO | SMB | Enterprise | SP |

Functionality

The Cisco ASA 5500 Series Adaptive Security Appliance scales to meet a range of enterprise requirements and network sizes. The ASA 5500 Security Appliance family currently consists of three models: the ASA 5510, 5520, and 5540 Security Appliances. The ASA 5510 Security Appliance has integrated 10/100BASE-T ports. The ASA 5520 and 5540 Security Appliances support a single management 10/100 Fast Ethernet port and four Gigabit Ethernet ports. The ASA 5500 Adaptive Security Appliance models also support Secure Socket Layer (SSL) VPNs and an optional Advanced Inspection and Prevention Security Services Module (AIP-SSM).

The ASA Adaptive Security Appliance is secure right out of the box. After a few installation procedures and an initial configuration of six general commands, your ASA Adaptive Security Appliance is operational and protecting your network

Cisco PIX Firewall 501 Security Appliance

- **Designed for small offices and teleworkers**
- **7500 concurrent connections**
- **60-Mbps throughput**
- **Interface support**
  - **Supports one 10/100BASE-T* Ethernet interface (outside)**
  - **Has four-port 10/100 switch (inside)**
- **VPN throughput**
  - **3-Mbps 3DES**
  - **4.5-Mbps 128-bit AES**
- **Ten simultaneous VPN peers**

*100BASE-T speed option is available in release 6.3.

SNPA v4.0—2-5

The PIX 501 Security Appliance measures only 1.0 x 6.25 x 5.5 inches and weighs only 0.75 pounds, yet it delivers enterprise-class security for small offices and teleworkers. Ideal for securing high-speed, "always on" broadband environments, the PIX 501 Security Appliance delivers a multilayered defense for small office network environments through rich, integrated security services, including stateful inspection firewall services, advanced application and protocol inspection, site-to-site and remote access VPNs, intrusion prevention, and robust multimedia and voice security—all in a single, integrated solution.

The PIX 501 Security Appliance provides a convenient way for multiple computers to share a single broadband connection. In addition to its RJ-45 9600-baud console port and its integrated 10/100BASE-T port (100BASE-T option is available in Cisco PIX Security Appliance Software v6.3) for the outside interface, it features an integrated auto-sensing, auto-Medium Dependent Interface Crossover (MDIX) four-port 10/100 switch for the inside interface. Auto-MDIX support eliminates the need to use crossover cables with devices that are connected to the switch.

The PIX 501 Security Appliance can also secure all network communications from remote offices to corporate networks across the Internet using its standards-based Internet Key Exchange (IKE) and IPSec VPN capabilities. Users can also enjoy plug-and-play networking by taking advantage of the built-in Dynamic Host Configuration Protocol (DHCP) server within the PIX Security Appliance, which automatically assigns network addresses to the computers when they are powered on.

With PIX Security Appliance Software v6.3, there are several product licensing options available. Choose an appropriate user license. Each user license supports a maximum number of concurrent source IP addresses from the internal network to traverse through the PIX 501 Security Appliance. One can choose between a 10-user, 50-user, or unlimited-user license. For VPN encryption, there are two options: Data Encryption Standard (DES), which supports 56-bit DES encryption, or Triple DES (3DES), which supports both 168-bit 3DES and up to 256-bit Advanced Encryption Standard (AES) encryption. Software licensing is covered in greater detail later in this lesson.

The PIX 501 Security Appliance comes with an integrated security lock slot for improved physical security and contains 8 MB of Flash memory.

Note	The cable lock for the security lock slot is not provided with the firewall.

Note	The Cisco PIX 501 Security Appliance requires Cisco PIX Security Appliance Software v6.1(1) or higher.

Note	Prior to Cisco PIX Security Appliance Software v6.3, the outside interface was a half-duplex 10BASE-T Ethernet interface. With release 6.3, the outside interface can be configured for half- or full-duplex and 10BASE-T or 100BASE-T. Enabling this feature requires an upgrade to release 6.3.

Note	PIX 501 Security Appliance does not support Cisco PIX and ASA Security Appliance Software v7.0.

PIX Firewall 501: Front Panel LEDs
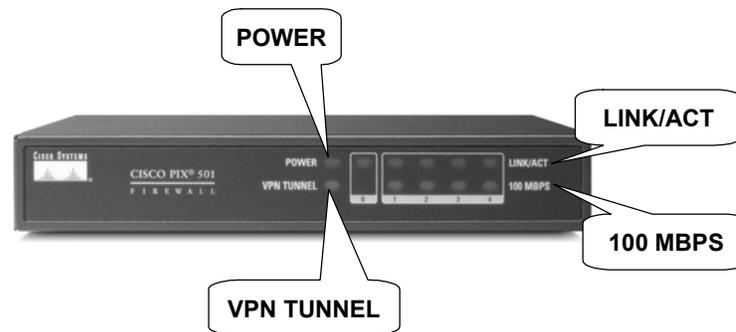
SNPA v4.0—2-6

The behavior of the light emitting diodes (LEDs) on the front panel of the PIX 501 Security Appliance is described here:

- POWER: When the device is powered on, the light is green.

- LINK/ACT(ivity): When the light is flashing green, network activity (such as Internet access) is present. When the light is green, the correct cable is in use and the connected equipment has power and is operational. When the light is off, no link is established.

- 100 MBPS: When the light is green, the interface is enabled at 100 Mbps (autonegotiated). When the light is off, the interface is enabled at 10 Mbps.

- VPN TUNNEL: When the light is green, one or more IKE/IPSec VPN tunnels are established. When the light is off, one or more IKE/IPSec VPN tunnels are disabled. If the standard configuration has not been modified to support VPN tunnels, the LED does not light up because it is disabled by default.

| **Note** | The VPN TUNNEL LED does not light up when Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP) tunnels are established. |

PIX Firewall 501: Back Panel

Cisco.com

Four-Port 10/100 Switch (RJ-45)

Console Port (RJ-45)

Security Lock Slot

10/100BASE-T (RJ-45)

Power Connector

POWER

© 2005 Cisco Systems, Inc. All rights reserved.

SNPA v4.0—2-7

This figure shows the back panel of the PIX 501 Security Appliance. The following describes the ports and other features:

■ Four-port 10/100 switch (RJ-45): Ports in the auto-sensing, auto-MDIX switch used for the inside interface. Connect your PC or other network devices to one of the four switched ports, which are numbered 1 through 4.

■ 10/100BASE-T port (100BASE-T option is available in Cisco PIX Security Appliance Software v6.3): Port 0, a half- or full-duplex Ethernet port for the public network. The PIX 501 Security Appliance comes with a yellow Ethernet cable (72-1482-01) and an orange Ethernet cable (72-3515-01). Use the yellow cable to connect the device to a switch or hub. Use the orange cable to connect the device to a DSL modem, cable modem, or router.

■ Console port: RJ-45 9600-baud console port used to connect a computer to the PIX Security Appliance for console operations.

■ Power connector: Used to attach the power supply cable to the PIX Security Appliance. The PIX 501 Security Appliance does not have a power switch.

■ Security lock slot: A slot that accepts standard desktop cable locks to provide physical security for small portable equipment, such as laptop computers.

Note When installing the PIX 501 Security Appliance, place the chassis on a flat, stable surface. The chassis is not rack mountable.

Note Prior to Cisco PIX Security Appliance Software v6.3, the outside interface was a half-duplex 10BASE-T Ethernet interface. With release 6.3, the outside interface can be configured for half- or full-duplex and 10BASE-T or 100BASE-T. Enabling this feature requires an upgrade to release 6.3.

PIX Firewall 506E Security Appliance

Cisco.com

- **Is designed for remote offices and small- to medium-sized businesses**
- **Provides 25,000 concurrent connections**
- **Provides 100-Mbps clear text throughput**
- **Supports Two interfaces**
  - **10/100BASE-T***
  - **Two VLANs***
- **Provides VPN throughput**
  - **17-Mbps 3DES**
  - **30-Mbps 128-bit AES**
- **Provides 25 simultaneous VPN peers**

*100BASE-T speed option is available in PIX Firewall Security Appliance Software v6.3 for 506E only. Two VLANs are supported in release 6.3(4).

SNPA v4.0—2-8

The Cisco PIX 506E Security Appliance delivers enterprise-class security for remote office, branch office, and small- to medium-sized business networks, in a high-performance, easy-to-deploy purpose-built appliance. Its unique desktop design supports two 10/100 Fast Ethernet interfaces and two 802.1q-based virtual interfaces, making it an exceptional choice for businesses requiring a cost-effective security solution with Demilitarized Zone (DMZ) support. The Cisco PIX 506E Security Appliance delivers a multilayered defense for remote office, branch office, and small- to medium-sized business network environments through rich, integrated security services, including stateful inspection firewall services, advanced application and protocol inspection, site-to-site and remote access VPNs, intrusion prevention, and robust multimedia and voice security—all in a single, integrated solution.

Cisco PIX 506E Security Appliance license is provided in a single, unlimited-user license. With PIX 506E Security Appliance, there are two VPN encryption options: DES, which supports 56-bit DES encryption, and 3DES, which supports both 168-bit 3DES and up to 256-bit AES encryption. Software licensing is covered in greater detail later in this lesson.

Note	100BASE-T port speed is available beginning with Cisco PIX Security Appliance Software v6.3. Prior to release 6.3, the PIX 506E Security Appliance supported a port speed of 10BASE-T only. The 100BASE-T performance upgrade is software-based. No PIX Security Appliance hardware upgrade is necessary. Beginning with Cisco PIX Security Appliance Software v6.3(4), PIX 506E Security Appliance supports two VLANs.

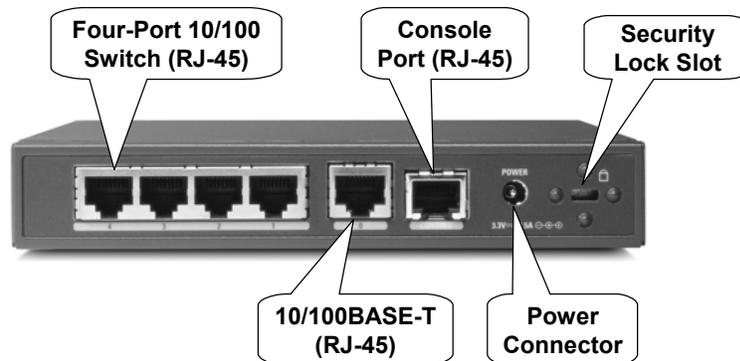|	
Note	The PIX 506 and 506E Security Appliances do not support Cisco PIX and ASA Security Appliance Software v7.0.

PIX Firewall 506E: Front Panel LEDs
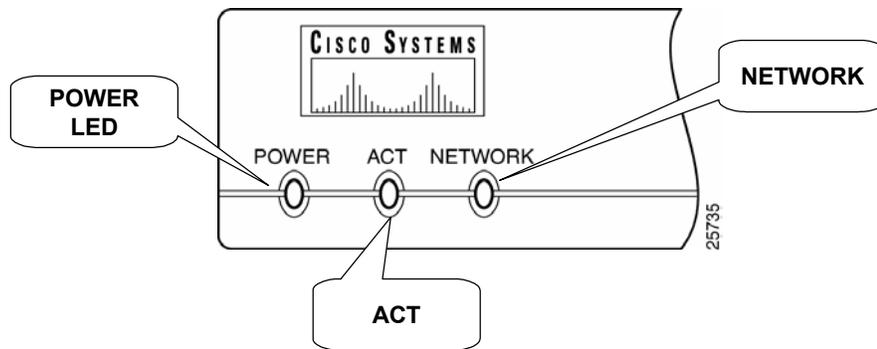
The behavior of the LEDs on the front panel of the PIX 506E Security Appliance is described here:

- POWER: When the device is powered on, the light is green.
- ACT(ive): When the software image has been loaded on the PIX 506E Security Appliance, the light is green.
- NETWORK: When at least one network interface is passing traffic, the light is green.

PIX Firewall 506E: Back Panel

Cisco.com

ACT LED, LINK LED, ACT LED, LINK LED, Power Switch

10/100BASE-T (RJ-45), USB Port

10/100BASE-T (RJ-45), Console Port (RJ-45)
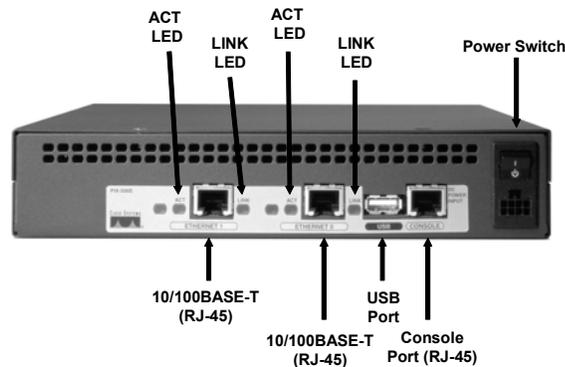
SNPA v4.0—2-10

On the PIX 506E Security Appliance, Ethernet1 connects the inside and DMZ networks using VLANs, and Ethernet0 is for the outside network. Use the console port to connect a computer to enter configuration commands. The USB port to the left of the console port is not used.

The power connection is directly beneath the power switch. The PIX 506E Security Appliance uses an external AC-to-DC power supply.

The LEDs on the back panel of the PIX 506E Security Appliance display the following transmission states:

■ ACT(ivity): Shows network activity.

■ LINK: Shows that data is passing on the network to which the connector is attached.

Note	100BASE-T port speed is available beginning with Cisco PIX Security Appliance Software v6.3. Prior to release 6.3, the PIX 506E Security Appliance supported a port speed of 10BASE-T only. The 100BASE-T performance upgrade is software-based. No PIX Security Appliance hardware upgrade is necessary. Starting with software release 6.3(4), PIX 506E Security Appliance supports two VLANs.

PIX Firewall 515E Security Appliance

- **Is designed for small- to medium-sized businesses and enterprise networks**
- **Provides 130,000 concurrent connections**
- **Provides 190-Mbps clear text throughput**
- **Provides Interface support**
  - **Up to six 10/100 Fast Ethernet interfaces**
  - **Up to 25 VLANs**
  - **Up to five contexts**
- **Supports failover**
  - **Active/standby**
  - **Active/active**
- **Supports VPNs (2,000 tunnels)**
  - **Site to site**
  - **Remote access**

SNPA v4.0—2-11

The Cisco PIX 515E Security Appliance delivers enterprise-class security for small- to medium-sized business and enterprise networks, in a modular, purpose-built appliance. Its versatile one-rack-unit (1RU) design supports up to six 10/100 Fast Ethernet interfaces, making it an excellent choice for businesses that require a cost-effective, resilient security solution with DMZ support.

The PIX 515E Security Appliance delivers a multilayered defense for small- to medium-sized business and enterprise networks through rich integrated security services, including stateful inspection firewalling, advanced application and protocol inspection, VPNs, intrusion detection, and robust multimedia and voice security—all in a single, integrated solution.

The PIX 515E Security Appliance supports up to six 10/100 Ethernet ports. This allows for more robust traffic configurations and establishes a protected DMZ for hosting a website or performing URL filtering and virus detection. With the restricted license, it supports three interfaces and ten VLANs; with the unrestricted license (UR license), it supports six interfaces, 25 VLANS, and up to five security contexts. Software licensing and security contexts are covered in greater detail later in this lesson.

This model also features integrated hardware-based IPSec acceleration, delivering VPN performance of up to 130 Mbps while freeing system resources for other mission-critical security functions. IPSec acceleration is provided by an integrated PIX Security Appliance VAC+ or the PIX Security Appliance VAC. VAC and VAC+ are covered in greater detail later in this lesson.

The PIX 515E Security Appliance is rack-mountable, comes with 16 MB of Flash memory, and uses Trivial File Transfer Protocol (TFTP) for image download and upgrade.

Note When a PIX 515E Security Appliance is ordered, the order automatically includes a VAC+ unless specified otherwise.

Note	A software upgrade in the PIX 515E from Cisco PIX Security Appliance Software v6.3 to Cisco PIX and ASA Security Appliance Software v7.0 requires a memory upgrade in the PIX 515E, from 32 MB to 64 MB in the security appliances with a restricted license and from 64 MB to128 MB in those with a UR license.

PIX Firewall 515E: Front Panel LEDs

Cisco.com

POWER

ACT

NETWORK

POWER   ACT   NETWORK

25735

SNPA v4.0—2-12
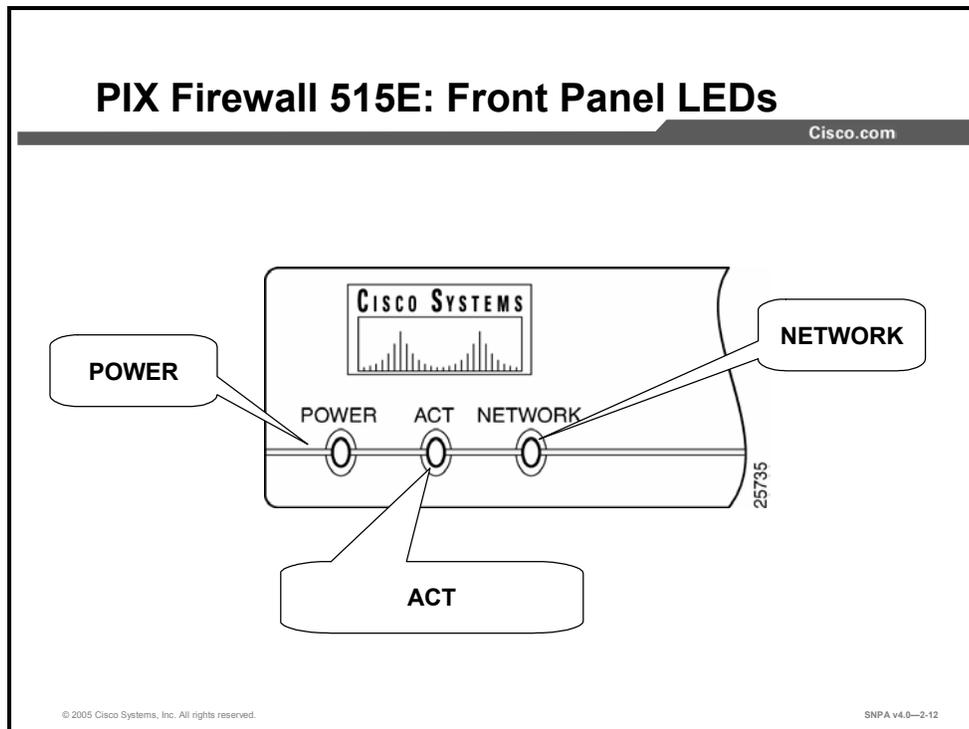
The behavior of the LEDs on the front panel of the PIX 515E Security Appliance is described here:

■ POWER: When the device is powered on, the light is green.

■ ACT(ive): When the PIX Security Appliance is used in a standalone configuration, the light is green. When the PIX Security Appliance is configured for failover operations, the light is green on the active PIX Security Appliance.

■ NETWORK: The light is green when at least one network interface is passing traffic.

PIX Firewall 515E: Back Panel
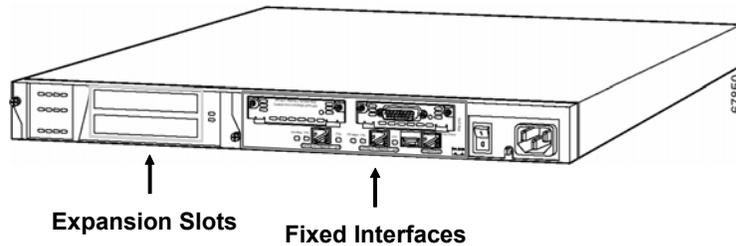
Expansion Slots   Fixed Interfaces

SNPA v4.0—2-13

The PIX 515E Security Appliance back panel can be logically divided into two sections, fixed interfaces and expansion slots. The fixed interfaces provide two 10/100BASE-TX Ethernet ports, a console port and a failover connector. The expansion slots provide two 32-bit 33-MHz protocol control information (PCI) slots. These PCI slots support easy installation of additional network interfaces and VAC or VAC+. Fixed interfaces and expansion slot option cards are covered in greater detail later in this lesson.

PIX Firewall 515E: Fixed Interface Connectors
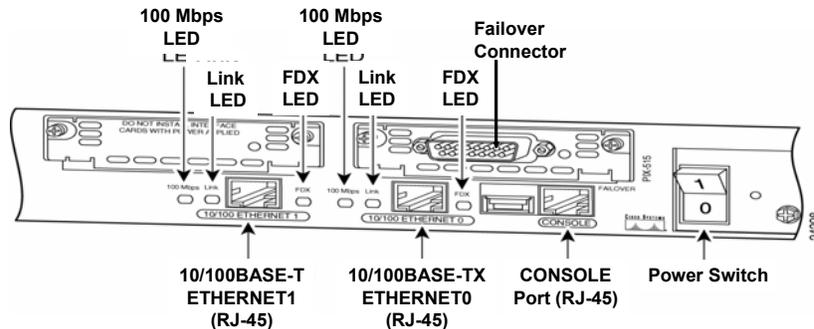
This figure shows the fixed interfaces of the PIX 515E Security Appliance. The following describes the ports, LEDs, and other fixed interface features:

■ Ethernet connections: With software versions 5.2 and higher, any port, whether a fixed port or a PCI expansion port, and any interface type can be assigned to be the inside or outside network port.

■ Console port: Used to connect a computer to the PIX Security Appliance for console operations.

■ Failover connection: Used to attach a failover cable between two PIX Security Appliances.

■ 100 Mbps LED: 100-Mbps, 100BASE-TX communication for the respective connector. If the light is off, the PIX 515E Security Appliance uses 10-Mbps data exchange.

■ Link LED: Indicates that data is passing on the network to which the connector is attached.

■ FDX LED: Indicates that the connection uses full-duplex data exchange (data can be transmitted and received simultaneously). If the light is off, half-duplex is in effect.

■ Power switch: Controls the power to the PIX Security Appliance.

Note   The USB port to the left of the console port and the detachable plate above the Ethernet1 connector are for future PIX Security Appliance enhancements.

PIX Firewall 515E: Expansion Slot Option Cards

Cisco.com

Expansion Slots
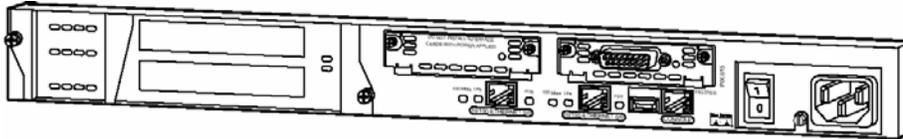
Fast Ethernet

VPN Accelerator

1FE   **4 FE - 66**   **VAC**   **VAC+**

SNPA v4.0—2-15

The two expansion slots support Fast Ethernet expansion option cards and hardware VACs. The features of both cards are as follows:

■ Fast Ethernet expansion option cards: Support the easy installation of additional network interfaces. The Fast Ethernet expansion option cards include single-port (1FE) and four-port Fast Ethernet (4FE) cards. The 4FE interface card delivers increased port density for each PCI slot. There are two versions of the 4FE card. The 4FE card operates at 33-MHz. The 4FE-66 card is a higher performance card that operates at 66-MHz. With the restricted license, the PIX 515E Security Appliance supports one additional expansion network port. With the UR license, the PIX 515E Security Appliance supports up to four additional expansion network ports.

■ Hardware VACs: Deliver high-performance VPN services via support of VAC and VAC+. The hardware-based VAC and VAC+ handle the voluminous mathematical functions required for IPSec. Offloading encryption functions to the VAC and VAC+ improves IPSec encryption processing. The VAC provides 56-bit DES and 168-bit 3DES encryption. The VAC has a 32-bit, 33-MHz PCI interface. The VAC+, in addition to supporting DES and 3DES, also provides 128-, 192-, and 256-bit AES encryption. The VAC+ has a 64-bit, 66-MHz PCI interface. The VAC+ is supported in Cisco PIX Security Appliance Software v6.3(1) or later. VAC and VAC+ are limited to one card per 515E, 525, and 535 chassis.

PIX Firewall 515E: Fast Ethernet Card Port Numbering

Single-port Card

Ethernet 2

Ethernet 3

Quad-port Card

Ethernet 5

Ethernet 3

Ethernet 2

Ethernet 4
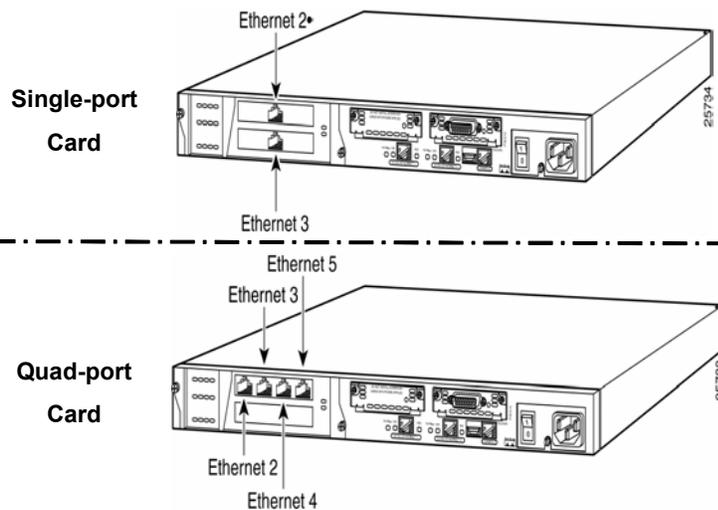
• **PIX Firewall 515E Security Appliance option cards require the UR license.**

© 2005 Cisco Systems, Inc. All rights reserved.   SNPA v4.0—2-16

If one or two 1FE cards are installed in the auxiliary assembly at the left rear of the PIX Security Appliance, the cards are numbered top to bottom; therefore, the top card is Ethernet2 and the bottom card is Ethernet3.

The quad-port card is a 4FE card. When you connect the perimeter network cables to this card, you begin with the far left connector and move right. For example, Ethernet2 will go in the far left connector, Ethernet3 in the second connector from the left, and so on.

Note	The maximum number of allowed interfaces is six. Additional interfaces will not be recognized.

- **Is designed for enterprise networks**
- **Provides 280,000 concurrent connections**
- **Provides 330-Mbps clear text throughput**
- **Provides Interface support**
  - **Up to ten 10/100 Fast Ethernet interfaces**
  - **Up to 100 VLANs**
  - **Up to 50 contexts**
- **Supports failover**
  - **Active/standby**
  - **Active/active**
- **Supports VPNs (2,000 tunnels)**
  - **Site to site**
  - **Remote access**

The Cisco PIX 525 Security Appliance delivers enterprise-class security for medium- to large-sized enterprise networks, in a reliable, purpose-built appliance. Its modular two-rack-unit (2RU) design incorporates two 10/100 Fast Ethernet interfaces and supports a combination of additional 10/100 Fast Ethernet interfaces and Gigabit Ethernet interfaces, making it an ideal choice for businesses requiring a high-performance, Gigabit Ethernet-ready solution that provides solid investment protection. With the restricted license, it supports up to six interfaces and 25 VLANs; with the UR license, it supports up to ten interfaces, 100 VLANs, and 50 security contexts. Software licensing is covered in greater detail later in this lesson.

The Cisco PIX 525 Security Appliance delivers a multilayered defense for medium- to large-sized enterprise networks through rich, integrated security services, including stateful inspection firewall services, advanced application and protocol inspection, site-to-site and remote access VPN, intrusion detection, and robust multimedia and voice security—all in a single, integrated solution.

The PIX 525 Security Appliance also offers multiple power supply options. You can choose between an AC and a 48-DC power supply. Either option can be paired with a second power supply for redundancy and high availability.

Note	Currently, a VAC+ is included with every PIX 525 Security Appliance ordered unless otherwise specified.
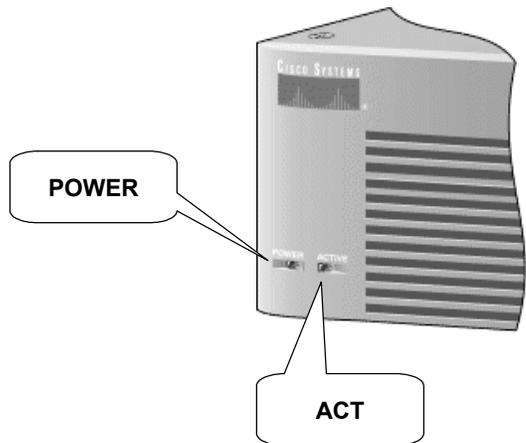
There are two LEDs on the front panel of the PIX 525 Security Appliance. The LEDs function as follows:

■ POWER: When the device is powered on, the light is green.

■ ACT(ive): The light is on when the PIX Security Appliance is the active failover firewall. If failover is configured, the light is on when the PIX Security Appliance is the active firewall and off when it is in standby mode.

PIX Firewall 525: Back Panel
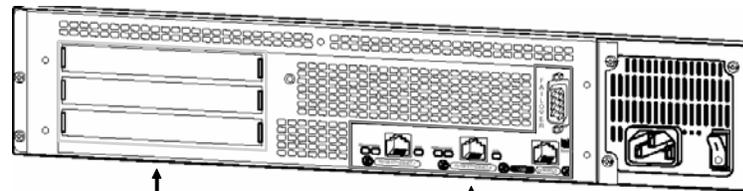
Expansion Slots

Fixed Interfaces

SNPA v4.0—2-19

The PIX 525 Security Appliance back panel can be logically divided into two sections, fixed interfaces and expansion slots. The fixed interfaces provide two 10/100BASE-TX Ethernet ports, a console port and a failover connector. The expansion slots provide three 32-bit 33-MHz PCI slots. These PCI slots support easy installation of additional network interfaces and a VAC or VAC+. Fixed interfaces and expansion slot option cards are covered in greater detail later in this lesson.

PIX Firewall 525: Fixed Interface Connectors
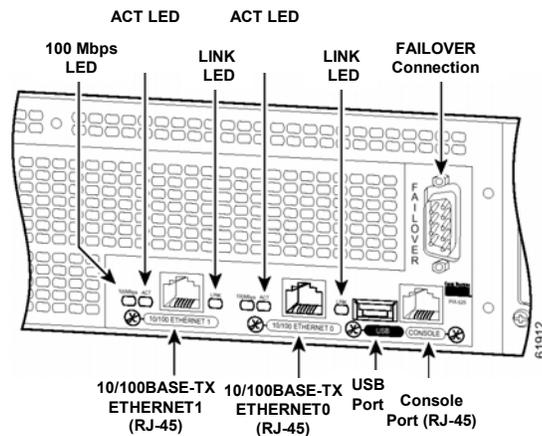
SNPA v4.0—2-20

On the back of the PIX 525 Security Appliance, there are three LEDs for each RJ-45 interface port and three types of fixed interface connectors. The LEDs display the following transmission states:

■ 100 Mbps: 100-Mbps, 100BASE-TX communication. If the light is off during network activity, that port is using 10-Mbps data exchange.

■ ACT(ivity): Shows network activity.

■ LINK: Shows that data is passing through that interface.

The following are fixed connectors on the back of the PIX 525 Security Appliance:

■ RJ-45: Network and console connectors

■ DB-15: Failover cable connector

■ USB: Not used at the present time

The inside, outside, and perimeter network connections can be made to any available interface port on the PIX 525 Security Appliance. If you are using only the Ethernet0 and Ethernet1 ports, connect the inside network cable to the interface connector marked Ethernet0 or Ethernet1. Connect the outside network cable to the remaining Ethernet port.

PIX Firewall 525: Expansion Cards and VACs
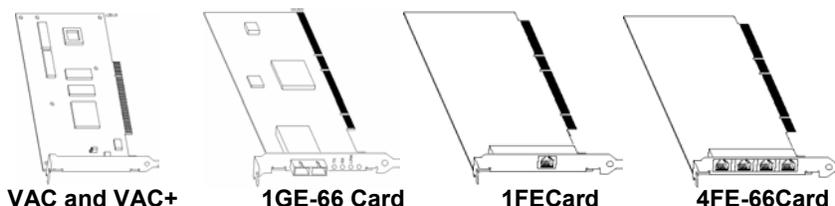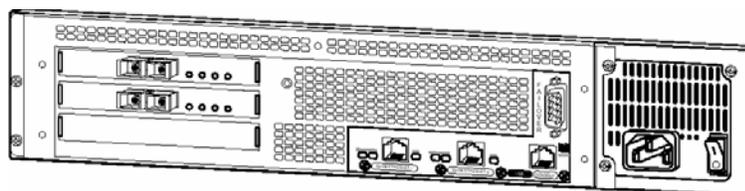
VAC and VAC+   **1GE-66 Card**   **1FECard**   **4FE-66Card**

SNPA v4.0—2-21

The PIX 525 Security Appliance supports easy installation of additional network interfaces via three PCI expansion slots. The expansions cards it supports include 1FE, 4FE, single-port Gigabit Ethernet (1GE), VAC, and VAC+.The"-66" denotes a card clock speed of 66 MHz.

A maximum of six interfaces are supported with a restricted license, and a maximum of ten interfaces are possible with the UR license. Currently, a VAC+ card is included with every PIX 525 Security Appliance unless otherwise specified.

When connecting the network cables to the expansion interface ports, use the following guidelines: The first expansion port number, at the top left, is interface 2. Starting from that port and going from left to right and top to bottom, the next port is interface 3, the next is interface 4, and so on.

PIX Firewall 535 Security Appliance

- **Is designed for enterprise and service providers**
- **Provides 500,000 concurrent connections**
- **Provides 1.65-Gbps clear text throughput**
- **Provides Interface support**
  - **Up to 14 Fast and Gigabit Ethernet interfaces**
  - **Up to 150 VLANs**
  - **Up to 50 contexts**
- **Supports failover**
  - **Active/standby**
  - **Active/active**
- **Supports VPNs (2,000 tunnels)**
  - **Site to site**
  - **Remote access**

SNPA v4.0—2-22

The Cisco PIX 535 Security Appliance delivers enterprise-class security for large enterprise and service provider networks, in a high-performance, purpose-built appliance. Its highly modular three-rack-unit (3RU) design supports a combination of 10/100 Fast Ethernet interfaces and Gigabit Ethernet interfaces, integrated VAC, and redundant power supplies, making it an ideal choice for businesses that require the highest levels of performance, port density, reliability, and investment protection. With the restricted license, the PIX 535 Security Appliance supports up to eight interfaces and 50 VLANs; with the UR license, it supports up to 14 interfaces, 150 VLANs, and 50 security contexts. Software licensing is covered in greater detail later in this lesson.

The Cisco PIX 535 Security Appliance delivers a multilayered defense for large enterprise and service provider networks through rich, integrated security services, including stateful inspection firewall services, advanced application and protocol inspection, site-to-site and remote access VPN, intrusion detection, and robust multimedia and voice security—all in a single, integrated solution. It has a throughput of 1.65 Gbps with the ability to handle up to 500,000 concurrent connections and 2,000 IPSec tunnels.

Note	If you configure a PIX Security Appliance for Gigabit Ethernet cards and later replace the cards with 10/100 Ethernet cards, the order of the cards in the configuration changes from what you originally configured. For example, if you configure Ethernet0 for a Gigabit Ethernet card that is assigned to the inside interface and later replace this card with a 10/100 Ethernet card, the card may no longer appear as Ethernet0.

The PIX 535 Security Appliance comes with 16 MB of Flash memory and supports the Cisco PIX Security Appliance Software v5.3 or later.

Note	Currently, a VAC+ is included with every PIX 535 Security Appliance unless otherwise specified.

PIX 535: Front Panel LEDs

POWER

ACTIVE

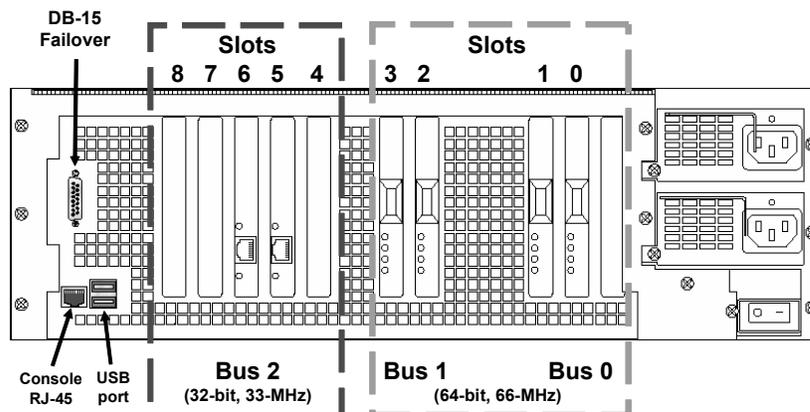SNPA v4.0—2-23

There are two LEDs on the front panel of the PIX 535 Security Appliance. The LEDs function as follows:

- POWER: When the device is powered on, the light is green.
- ACTIVE: The light is on when the PIX Security Appliance is the active failover firewall. If failover is present, the light is on when the PIX Security Appliance is the active firewall and off when it is in standby mode.

PIX 535: Back Panel

Cisco.com

DB-15 Failover

Slots 8 7 6 5 4

Slots 3 2 1 0

Console RJ-45   USB port

Bus 2 (32-bit, 33-MHz)

Bus 1   Bus 0 (64-bit, 66-MHz)

SNPA v4.0—2-24

There are three separate buses for the nine interface slots in the PIX 535 Security Appliance. The figure is a reference for the interface slot configuration on the PIX 535 Security Appliance.

The slots and buses are configured as follows:

- Slots 0 and 1: 64-bit, 66-MHz bus 0

- Slots 2 and 3: 64-bit, 66-MHz bus 1

- Slots 4 through 8: 32-bit, 33-MHz bus 2

The PIX 535 Security Appliance expansion port function is dependent on three factors: PIX software license, expansion card PCI bus interface, and PIX 535 Security Appliance slot bus speed. A description of each item is as follows:

- Software license: A maximum of eight interfaces are supported with a restricted license, and a maximum of 14 interfaces are possible with a UR license.

- Expansion card PCI bus interface: An expansion card ships with either a 32-bit, 33-MHz or 64-bit, 66-MHz PCI interface. The 64-bit, 66-MHz PCI bus interface card delivers potentially higher throughput. The 64-bit, 66-MHz PCI bus interface cards are backward-compatible with the PIX Security Appliance 32-bit, 33-MHz expansion slots.

- Slot bus speed: A PIX 535 Security Appliance has two different bus configurations. Bus 0 and bus 1 are configured for a 64-bit, 66-MHz interface. Bus 2 is configured for a 32-bit, 33-MHz interface.

PIX Firewall 535: Option Cards

Gigabit Ethernet

1GE

1GE-66

Fast Ethernet

1FE

4FE-66

VPN Accelerator

VAC

VAC+

4FE
(EOS)

SNPA v4.0—2-25

There are three types of options cards available for the PIX 535 Security Appliance: 1GE; 1FE and 4FE; and VAC and VAC+. Notice that for most card types, there is a 33-MHz and a 66-MHz version. For example, the 1GE card has a 33-MHz PCI interface. The 1GE-66 card has a 66-MHz PCI interface. There are also the nine interface slots and three buses in the PIX 535 Security Appliance.
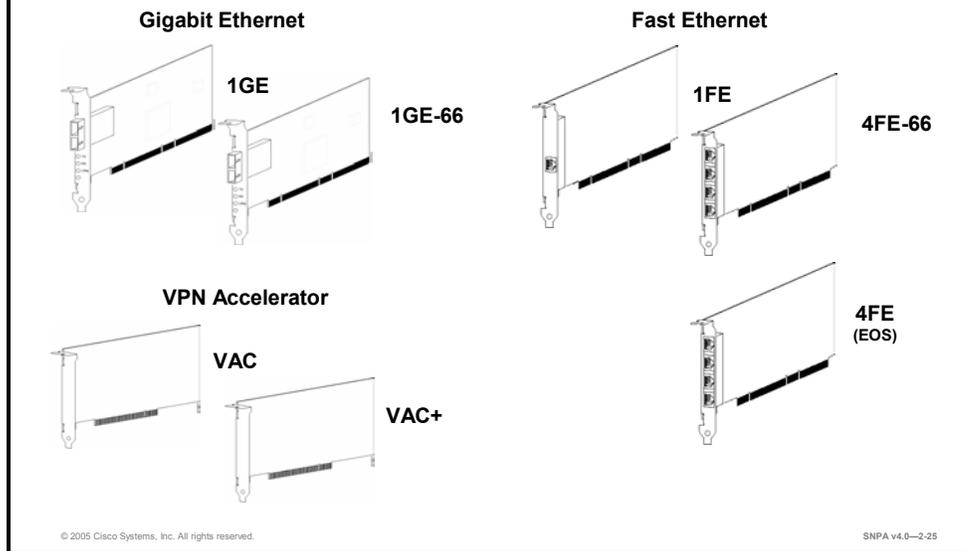
The slots and buses are configured as follows:

- Slots 0 and 1: 64-bit, 66-MHz bus 0
- Slots 2 and 3: 64-bit, 66-MHz bus 1
- Slots 4 to 8: 32-bit, 33-MHz bus 2

For optimum performance and throughput for the interface circuit boards, use the following guidelines:

- A total of eight interfaces are configurable on the PIX 535 Security Appliance with the restricted license, and a total of fourteen are configurable with the UR license.
- For best performance, the 1GE-66, 4FE-66, and VAC+ (66 MHz) circuit boards should be installed in a 64-bit, 66-MHz card slot. Performance will be degraded if this recommendation is not followed.
- The 1GE, 1FE, 4FE, and VAC (33 MHz) circuit boards should be installed in the 32-bit, 33-MHz card slots.

Note   The 1GE circuit board is not recommended for use in the PIX 535 Security Appliance because it can severely degrade performance. It is capable of only half the throughput of the 1GE-66 circuit board. If the 1GE circuit board is detected in the PIX 535 Security Appliance, a warning about degraded performance will be issued.

- The 4FE card (end of sale: July 2003) can be installed only in a 32-bit, 33-MHz card slot and must never be installed in a 64-bit, 66-MHz card slot. Installation of this circuit board in a 64-bit, 66-MHz card slot can cause the system to hang at boot time.

- The 1FE circuit board (33 MHz) can be installed in any bus or slot (32-bit, 33-MHz or 64-bit, 66-MHz). Up to nine 1FE circuit boards or up to two 4FE circuit boards can be installed. The 1FE circuit boards should be installed in the 32-bit, 33-MHz card slots first.

- Do not mix the 1FE circuit boards with the 1GE-66 circuit boards on the same 64-bit, 66-MHz bus (bus 0 or bus 1). The overall speed of the bus is reduced by the lower-speed circuit board.

- If stateful failover is enabled for 1GE-66 traffic, the failover link must be PIX-1GE-66. The amount of stateful failover information is proportional to the amount of traffic flowing through the PIX Security Appliance, and if it is not configured properly, loss of state information or 256-byte block depletion can occur.

PIX 535: Back Panel

Cisco.com

DB-15
Failover

USB
Port

Slot 8 Slot 6   Slot 4   Slot 2   Slot 1

Console   Slot 7 Slot 5   Slot 3   Slot 0
RJ-45
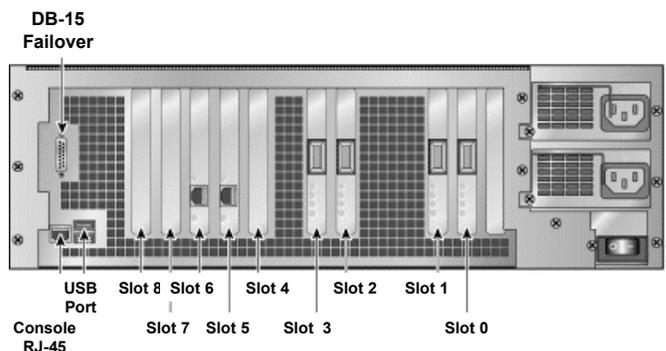
SNPA v4.0—2-26

Depending upon the type of interface, there are four possible LEDs for each network interface port. The LEDs for the network interface ports display the following transmission states:

- 100-Mbps: 100-Mbps 100BASE-TX communication. If the light is off during network activity, that port is using 10-Mbps data exchange.

- ACT: Shows network activity.

- LINK: Shows that data is passing through that interface.

- FDX: Shows that the connection uses full-duplex data exchange, that is, data can be transmitted and received simultaneously. If this light is off, half-duplex is in effect.

When connecting the inside, outside, or perimeter network cables to the interface ports on the PIX 535 Security Appliance, starting from the right and moving left, the connectors are Ethernet0, Ethernet1, Ethernet2, and so forth.

Note	The PIX 535 Security Appliance is equipped with hot-swappable power supplies. If a power supply fails, you can remove the power supply without powering off the PIX 535 Security Appliance.

Cisco ASA 5510 Adaptive Security Appliance

- **Delivers all-in-one enterprise, remote office, and small- to medium-sized business security and VPN gateway**
- **Provides 64,000 concurrent connections**
- **Provides 300-Mbps firewall throughput**
- **Provides interface support**
  - **Up to five 10/100 Fast Ethernet interfaces**
  - **Up to ten VLANs**
- **Supports failover**
  - **Active/standby**
- **Supports VPNs**
  - **Site to site**
  - **Remote access**
  - **WebVPN**
- **Supports AIP-SSM-10 (optional)**

SNPA v4.0—2-28

The Cisco ASA 5510 Adaptive Security Appliance delivers enterprise-class security for small-to medium-sized businesses and enterprise networks, in a reliable, purpose-built security appliance. Its modular 1RU design incorporates up to four 10/100 Fast Ethernet interfaces and one 10/100 Fast Ethernet management-only interface and has a slot for an optional security services module that provides inline intrusion prevention, making it an ideal choice for businesses requiring a high-performance, Fast Ethernet-ready solution that provides solid investment protection.

The ASA 5510 Security Appliance delivers a multilayered defense for enterprise networks through rich, integrated security services, including stateful inspection firewall services, advanced application and protocol inspection, site-to-site and remote access VPNs, WebVPN, intrusion prevention, and robust multimedia and voice security—all in a single, integrated solution. It has a throughput of 300 Mbps with the ability to handle up to 64,000 concurrent connections. It supports active/standby failover. It also supports site-to-site VPN, remote access VPN, and WebVPN applications. The ASA 5510 Security Appliance supports an optional AIP-SSM.

The ASA 5510 Security Appliance also offers multiple power supply options. You can choose between an AC and a 48-DC power supply.

Cisco ASA 5520 Adaptive Security Appliance

- **Delivers all-in-one enterprise and small- to medium-sized business headend security and VPN gateway**
- **Provides 130,000 concurrent connections**
- **Provides 450-Mbps firewall throughput**
- **Provides Interface support**
  - **Four 10/100/1000 Gigabit Ethernet interfaces**
  - **One 10/100 Fast Ethernet interface**
  - **Up to 25 VLANs**
  - **Up to 10 contexts**
- **Supports failover**
  - **Active/standby**
  - **Active/active**
- **Supports VPNs**
  - **Site to site**
  - **Remote access**
  - **WebVPN**
- **Supports AIP-SSM-10 (optional)**

SNPA v4.0—2-29

The Cisco ASA 5520 Adaptive Security Appliance delivers enterprise-class security for small-to medium-sized businesses and enterprise networks, in a reliable, purpose-built security appliance. Its modular 1RU design incorporates four 10/100/1000 Gigabit Ethernet interfaces and one 10/100 Ethernet Management interface, and it has a slot that supports an optional security services module that provides inline intrusion prevention, making it an ideal choice for businesses that require a high-performance, Gigabit Ethernet-ready solution that provides solid investment protection.

The ASA 5520 Security Appliance delivers a multilayered defense for enterprise networks through rich, integrated security services, including stateful inspection firewall services; advanced application and protocol inspection; site-to-site, remote access, and SSL VPNs; intrusion prevention; and robust multimedia and voice security—all in a single, integrated solution. It has a throughput of 450 Mbps with the ability to handle up to 130,000 concurrent connections. It supports active/standby and active/active failover and site-to-site VPN, remote access VPN, and WebVPN applications. The ASA 5520 Security Appliance supports an optional AIP-SSM.

The ASA 5520 Security Appliance also offers multiple power supply options. You can choose between an AC and a 48-DC power supply.

Cisco ASA 5540 Adaptive Security Appliance

Cisco.com

- **Delivers all-in-one enterprise and small-to medium-sized business headend security and VPN Gateway**
- **Provides 280,000 concurrent connections**
- **Provides 400-Mbps firewall throughput**
- **Provides Interface support**
  - **Four 10/100/1000 Gigabit Ethernet interfaces**
  - **One 10/100 Fast Ethernet interface**
  - **Up to 100 VLANs**
  - **Up to 50 contexts**
- **Supports failover**
  - **Active/standby**
  - **Active/active**
- **Supports VPNs**
  - **Site to site (5,000 peers)**
  - **Remote access**
  - **WebVPN**
- **Supports AIP-SSM-20 (optional)**

SNPA v4.0—2-30

The Cisco ASA 5540 Adaptive Security Appliance delivers enterprise-class security for enterprise networks, in a reliable, purpose-built security appliance. Its modular 1RU design incorporates four 10/100/1000 Gigabit Ethernet interfaces and one 10/100 Fast Ethernet management interface, and it has a slot that supports an optional security services module that provides inline intrusion prevention, making it an ideal choice for businesses that require a high-performance, Gigabit Ethernet-ready solution that provides solid investment protection.

The ASA 5540 Security Appliance provides delivers a multilayered defense for enterprise networks through rich, integrated security services, including stateful inspection firewall services, advanced application and protocol inspection, site-to-site, remote access, and SSL VPN, intrusion prevention, and robust multimedia and voice security—all in a single, integrated solution. It has a throughput of 400 Mbps with the ability to handle up to 280,000 concurrent connections. It supports active/standby and active/active failover, site-to-site, remote access, and Web VPN applications. The ASA 5540 Security Appliance supports an optional AIP-SSM.

The ASA 5540 Security Appliance also offers multiple power supply options. You can choose between an AC and a 48-DC power supply.

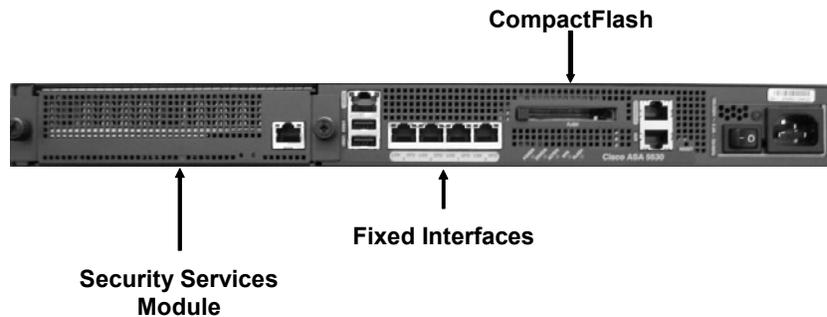# ASA 5500 Series: Front Panel

Cisco.com

STATUS FLASH

POWER ACTIVE VPN
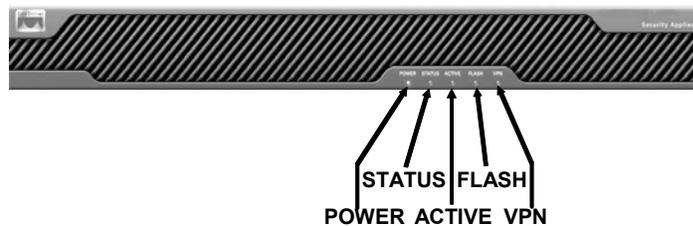
SNPA v4.0—2-31

The following describes the LEDs on the front panel of the ASA 5500 Series Adaptive Security Appliances:

- POWER: When the ASA Security Appliance is powered on, the light is green.

- STATUS: When the power-up diagnostics are running or the system is booting, the light flashes. When the system passes power-up diagnostics, the green light shines. When power-up diagnostics fail, the amber light shines.

- ACTIVE: When there is network activity, the light flashes.

- FLASH: When the CompactFlash memory is accessed, the light is green.

- VPN: When data is passing through the interface, the light is green.
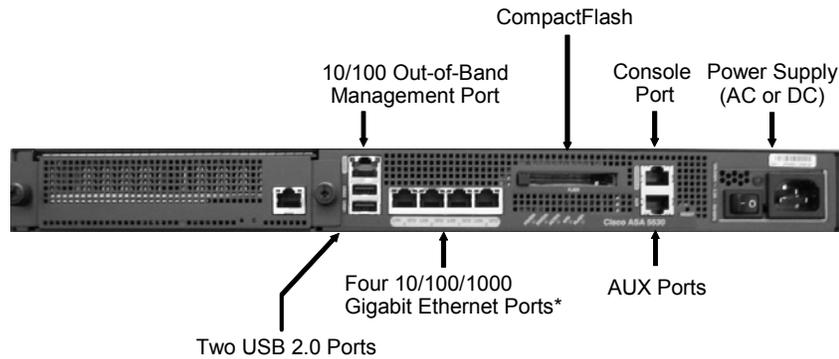
ASA 5500 Series: Back Panel

CompactFlash

Fixed Interfaces

Security Services Module

SNPA v4.0—2-32

The back panel of the ASA 5500 Series Adaptive Security Appliances can be logically divided into two sections, fixed interfaces and the slot for a security services module. The fixed interfaces on an ASA 5510 Security Appliance provide up to four 10/100 Fast Ethernet ports and one 10/100 Fast Ethernet management-only port. The ASA 5520 and 5540 Security Appliances provide four 10/100/1000 Gigabit Ethernet ports and one 10/100 Fast Ethernet port. In the ASA 5520 and 5540 Security Appliances, one 10/100 Fast Ethernet port can be used for management traffic or data traffic. The security services module slot enables other high-performance services to be added to the security appliance, such as the Cisco AIP-SSM.

ASA 5500 Series: Connectors

Cisco.com

CompactFlash

10/100 Out-of-Band
Management Port

Console
Port

Power Supply
(AC or DC)

Four 10/100/1000
Gigabit Ethernet Ports*

AUX Ports

Two USB 2.0 Ports

*ASA 5510 supports 10/100 Fast Ethernet ports.

SNPA v4.0—2-33

This figure shows the fixed interface connectors on the back panel of the ASA 5520 and 5540 Adaptive Security Appliances. These connectors are described here:

- Power supply: Supports either an AC or a DC power supply module

- Console port: Used to connect a computer to the ASA 5500 for console operations

- CompactFlash memory

- 10/100 Fast Ethernet out-of-band management port

- Two USB 2.0 ports: For future enhancements

- Four 10/100/1000 Gigabit Ethernet ports:

    — ASA 5510 supports four 10/100 Fast Ethernet ports

    — ASA 5520 and 5540 support four 10/100/1000 Gigabit Ethernet ports

- One 10/100 Fast Ethernet out of band management port:

    — For management only in ASA 5510

    — For either management or data traffic in ASA 5520 and 5540

- AUX port: For future enhancements

Security Services Module

- **High-performance module designed to provide additional security services**
- **Diskless (Flash-based) design for improved reliability**
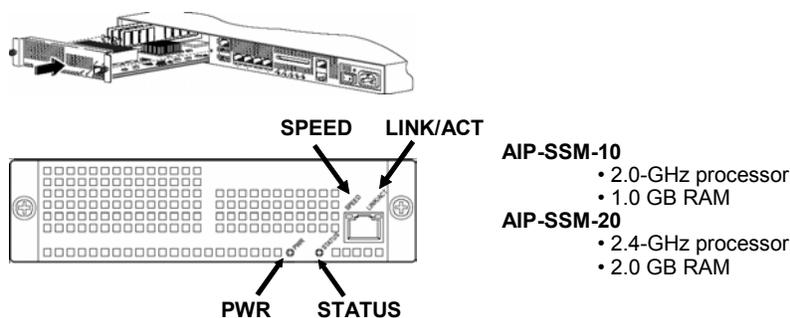- **Gigabit Ethernet port for out-of-band management**

SNPA v4.0—2-34

The Cisco ASA 5500 Series Adaptive Security Appliances deliver a wide range of features and a suite of security features. Firewall, IPSec, and SSL VPN services are provided on the security appliance. Additional security services are provided on the optional security services module plug-in hardware. Security services modules are high-performance modules based on a Pentium 4 Class processor. Diskless (Flash-based) design provides improved reliability. The current offering is an AIP-SSM card.

AIP-SSM

SPEED   LINK/ACT

AIP-SSM-10
- 2.0-GHz processor
- 1.0 GB RAM

AIP-SSM-20
- 2.4-GHz processor
- 2.0 GB RAM

PWR   STATUS

The AIP-SSM card is available in two versions: AIP-SSM-10 and AIP-SSM-20. The AIP-SSM can function in two modes, inline or promiscuous. In the inline mode, packets are sent to the AIP-SSM, inspected, then returned to the ASA Adaptive Security Appliance. Operating in inline mode puts the AIP-SSM directly into the traffic flow. In promiscuous mode, the AIP-SSM is not directly in the packet flow. The AIP-SSM performs analysis on a "copy" of the traffic instead of on the actual forwarded packet.

The following are AIP-SSM LEDs:

- PWR: When the AIP-SSM is powered on, the light is green.

- STATUS: When the power-up diagnostics are running or the system is booting, the light flashes. When the system passes power-up diagnostics, the light is steady green. When power-up diagnostics fail, the light is steady amber.

- SPEED: With 10 Mbps of traffic, the light is off. With 100 Mbps traffic, the light is green. With 1000 Mbps of traffic, the light is amber.

- LINK/ACT(ivity): When there is network activity, the light flashes.

PIX Security Appliance Licensing

This topic explains the licensing options for the Cisco PIX 500 Series Security Appliances.

PIX License Types

- **UR: Allows installation and use of the maximum number of interfaces and RAM supported by the platform.**
- **Restricted: Limits the number of interfaces supported and the amount of RAM available within the system (no contexts and no failover).**
- **Active/standby failure: Places one security appliance in a failover mode for use alongside a security appliance that has a UR license. Only one unit can be actively processing user traffic; the other unit acts as a hot standby.**
- **Active/active failover: Places a security appliance that has a UR license in a failover mode for use alongside another security appliance that has a UR license, or two UR licenses. Both units can actively process traffic while serving as a backup for each other.**

Applies to PIX Firewall 515/515E, 525, and 535

SNPA v4.0—2-37

Current security appliance licensing is a feature-based license key system. The security appliance license determines the level of service the security appliance provides, its functions in a network, and the maximum number of interfaces and memory it can support.

For the PIX 500 Series Security Appliances, the following licensing is available:

- PIX 501 Security Appliance: A 10-user, 50-user, or UR license is provided via PIX Security Appliance Software v6.3. Each license except the UR license allows a specified maximum number of concurrent source IP addresses from your internal network to traverse the firewall. For instance, the 50-user license allows up to 50 concurrent source IP addresses from your internal network to traverse the firewall. If a PIX 501 Security Appliance requires more concurrent users to traverse the security appliance, the following upgrades of user licenses are available: 10-user to 50-user license, 10-user to UR license, and 50-user to UR license.

- PIX 506E Security Appliance: A single UR license is provided.

- PIX 515E, 525, and 535 Security Appliances available with the following basic license types:

    — UR license: PIX Security Appliance platforms in a UR license mode allow installation and use of the maximum number of interfaces and RAM supported by the platform. The UR license supports failover.

    — Restricted license: PIX Security Appliance platforms in a restricted license mode limit the number of interfaces supported and the amount of RAM available within the system. A restricted licensed firewall does not support contexts or failover configurations.

— Active/standby failover: Places the PIX Security Appliance in a failover mode for use alongside a PIX Security Appliance that has a UR license. Only one unit can be actively processing user traffic; the other unit acts as a hot standby.

— Active/active failover: Places a PIX Security Appliance that has a UR license in a failover mode for use alongside another PIX Security Appliance that has a UR license. Both units can actively process firewall traffic while serving as a backup for each other. Active/active failover is supported using security contexts.

Cisco supplies an activation key with a license. The activation key is based on the type of license and the serial number of the security appliance. To enable the license features, enter the activation key into the security appliance configuration. Unlike the Cisco PIX Security Appliance Software v6.3, which always requires a valid license key to run, Cisco PIX and ASA Security Appliance Software v7.0 can run without a license key, but it runs in with the default settings. When upgrading from PIX Security Appliance v6.3 to PIX and ASA v7.0, the existing license key for release 6.3 is saved in a central location on the Flash file system. When downgrading from PIX and ASA v7.0 to PIX Security Appliance v6.2 or v6.3, the license key that was saved during the upgrade procedure is retrieved and saved to the PIX Security Appliance v6.2 or v6.3 image.

Note   An activation key is tied to a specific security appliance using the security appliance's serial number.

VPN Encryption License

- **DES license**
  - **Provides 56-bit DES**
- **3DES/AES license**
  - **Provides 168-bit 3DES**
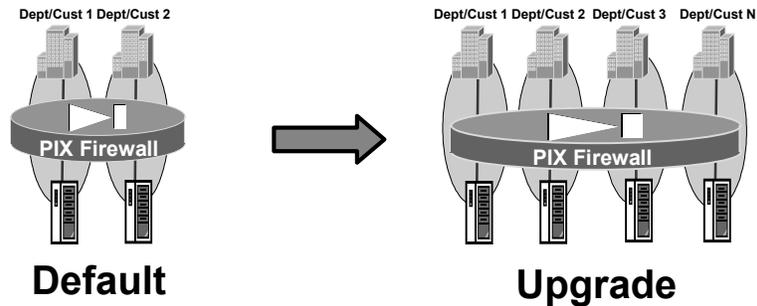 - **Provides up to 256-bit AES**

SNPA v4.0—2-38

Besides upgrading the security appliance license, you may wish to add data encryption services or increase the level of data encryption that your PIX Security Appliance can provide. You can complete an online form at Cisco.com to obtain a free 56-bit DES key. A separate form is required in order to install or upgrade to 168-bit 3DES encryption. For failover configurations, the UR and FO licenses each require their own unique corresponding DES or 3DES/AES license for failover functionality.

Adding cryptographic services and upgrading your security appliance license both require obtaining and installing an activation key. Log on to Cisco.com for current information on obtaining activation keys.

PIX Firewall Security Context Licenses

Dept/Cust 1 Dept/Cust 2

PIX Firewall

Default

Dept/Cust 1 Dept/Cust 2 Dept/Cust 3 Dept/Cust N

PIX Firewall

Upgrade

SNPA v4.0—2-39

You can partition a single UR-licensed PIX 515E, 525, or 535 Security Appliance into multiple virtual firewalls, known as security contexts. Each context is an independent firewall, with its own security policy, interfaces, and administrators. By default, two contexts are included in UR license. You may purchase an additional predetermined number of contexts. As your network grows or your requirements change, you may purchase an upgrade context license to increase the number of available contexts. The number of contexts available in a PIX Security Appliance is dependent upon the model and the context license. A PIX 515E Security Appliance supports up to five contexts, PIX 525 and 535 Security Appliances support up to 50 contexts.

PIX 515E, 525, and 535 Licensing

License Type	Physical Interfaces	VLANs	Contexts	Memory	Failover
PIX Firewall 515E					
Restricted	3	10	N/A	64	No
UR	6	25	License Up to five	128	Yes
PIX Firewall 525					
Restricted	6	25	N/A	128	No
UR	10	100	License Up to 50	256	Yes
PIX Firewall 535					
Restricted	8	50	N/A	512	No
UR	14	150	License Up to 50	1024	Yes

The table in the figure compares the restricted and UR licenses of the PIX 515E, 525, and 535 Security Appliances. For each license type and security appliance model, the table provides the maximum number of physical interfaces, the maximum number of VLANS, the maximum number of contexts, the RAM size, and failover capability.

ASA Adaptive Security Appliance Licensing

This topic explains the licensing options for the Cisco ASA 5500 Series Adaptive Security Appliances. Cisco ASA Security Appliance licensing is a feature-based license key system. The Cisco ASA Security Appliance license determines the number of contexts, the type of VPN encryption, and the number of VPN peers that an ASA Security Appliance can support.

ASA Security Context Licenses

Cisco.com

Default
- **Two contexts**

Available Context Licenses
- **Five contexts**
- **Ten contexts**
- **20 contexts**
- **50 contexts**

Upgrade Licenses
- **From Five to Ten contexts**
- **From Ten to 20 contexts**
- **From 20 to 50 contexts**
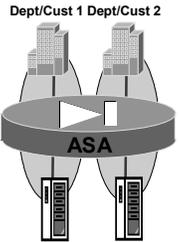
Dept/Cust 1 Dept/Cust 2

ASA

SNPA v4.0—2-42

The figure shows the licensing that is available for the Cisco ASA 5500 Series Security Appliances. You can partition a single ASA Security Appliance into multiple virtual firewalls, known as security contexts. Each context is an independent firewall, with its own security policy, interfaces, and administrators. By default, the ASA 5520 and 5540 Security Appliances support two contexts. You may purchase an initial context license for a predetermined number of contexts. As your network grows or your requirements change, you may also purchase an upgrade context license to increase the number of available contexts. The number of contexts available in an ASA Security Appliance is dependent upon the model and the context license. An ASA 5520 Security Appliance supports up to ten contexts, and an ASA 5540 Security Appliance supports up to 50 contexts.

ASA 5510, 5520, and 5540 Licensing

Licenses	Interfaces	Security Contexts	VLANs	IPSec VPN Peers	Failover A/S	Failover A/A	GPRS GTP
ASA 5510							
Base	3 x 10/100	N/A	0	50	N/A	N/A	N/A
Security+	5 x 10/100	N/A	10	150	Yes	N/A	N/A
ASA 5520							
Base	4 x 10/100/1000, 1 10/100	Default 2; up to 10	25	300	Yes	Yes	License
VPN+	4 x 10/100/1000, 1 10/100	Default 2; up to 10	25	750	Yes	Yes	License
ASA 5540							
Base	4 x 10/100/1000, 1 10/100	Default 2; up to 50	100	500	Yes	Yes	License
VPN+	4 x 10/100/1000, 1 10/100	Default 2; up to 50	100	2000	Yes	Yes	License
VPN Premium	4 x 10/100/1000, 1 10/100	Default 2; up to 50	100	5000	Yes	Yes	License

SNPA v4.0—2-43

The table in the figure compares the licenses offered for the Cisco ASA 5510 Adaptive Security Appliance, the ASA 5520 Security Appliance, and the ASA 5540 Security Appliance. For each license type and security appliance model, the table provides the maximum number of physical interfaces, the maximum number of security contexts, the maximum number of VLANS, the maximum number of IPSec VPN peers, failover capabilities, and General Packet Radio System (GPRS) Tunneling Protocol (GTP).

Cisco Firewall Services Module

This topic describes the Cisco Firewall Services Module (FWSM) for the Cisco Catalyst 6500 Switch and Cisco 7600 Series Internet Router.
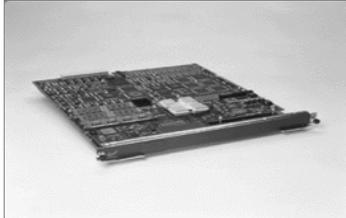
The FWSM is a multigigabit integrated firewall module for the Cisco Catalyst 6500 Series switch and the Cisco 7600 Series Internet Router. It is fabric-enabled and capable of interacting with the bus and the switch fabric. Based on PIX Security Appliance technology, the FWSM provides stateful firewall functionality in these switches and routers.

The following are the key features of the FWSM:

■ High-performance, 5-Gbps throughput, full-duplex firewall functionality

■ 5-Gbps throughput per module

■ Support for 1000 VLANs

■ 1 million concurrent connections

■ LAN failover—Active or standby, interchassis or intrachassis

■ Dynamic routing with Open Shortest Path First (OSPF) and passive Routing Information Protocol (RIP)

■ Supports up to four modules per chassis

The following table shows the major differences between the PIX Security Appliances and FWSM.

Comparison of FWSM and Security Appliances

	FWSM	Cisco Security Appliances I
Interfaces supported	1000 VLANs	150 VLANs
IPS functionality	Not present	Present
VPN functionality	Not present	Present
Performance	5 Gbps	1.65 Gbps

The FWSM comes with 128 MB of CompactFlash memory and 1 GB of DRAM memory. Memory is not field upgradable.

FWSM in Catalyst 6500 Switch and Cisco 7600 Internet Router

SNPA v4.0—2-46
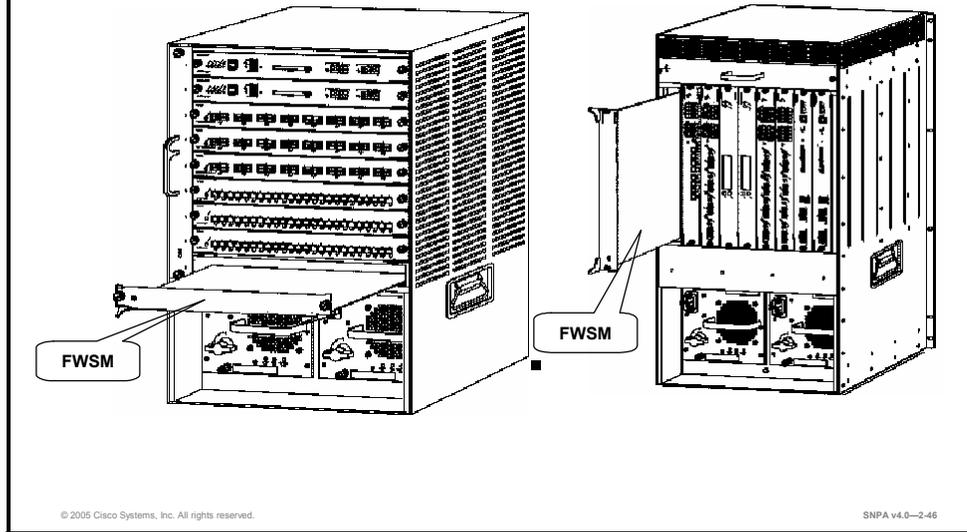
The figure shows the FWSM installed in slot 9 of a Catalyst 6500 nine-slot chassis and in slot 9 of a Cisco 7609 Internet Router. The Catalyst 6500 chassis and the Cisco 7609 Internet Router chassis can support up to four FWSM modules for a combined throughput of up to 20 Gbps per chassis.

| Note | Detailed instructions on installing a Catalyst 6500 Series Switch are provided in *Cisco Catalyst 6500 Advanced Switched Networks* (CACSN). The course introduces the Cisco Catalyst 6500 Series Switches, including a detailed overview of many of the modules and components. |

Summary

This topic summarizes what you learned in this lesson.

Summary

- **There are currently eight Cisco PIX Firewall and ASA Adaptive Security Appliance models.**
  - **In the Cisco 500 PIX Firewall Series: 501, 506E, 515E, 525, and 535**
  - **In the Cisco ASA 5500 Series: 5510, 5520 and 5540**
- **Your security appliance license determines the level of service and available features of your security appliance, and the number of interfaces it supports.**

SNPA v4.0—2-47

Summary (Cont.)

- **Restricted, unrestricted, and failover licenses are available for PIX Firewall Security Appliance models 515E, 525, and 535.**
- **The Cisco Firewall Services Module for the Cisco Catalyst 6500 Switches and the Cisco 7600 Series Internet Routers provides an alternative to the security appliance.**

SNPA v4.0—2-48

Lesson 3

Getting Started with Cisco Security Appliances

Overview

The purpose of this lesson is to teach the learner how to get started in configuring a security appliance. The lesson begins with describing the how to access the security appliance, then presents the basic commands that are needed to configure and monitor a security appliance.

Objectives

Upon completing this lesson, you will be able to configure the security appliance for basic network connectivity. This includes being able to meet these objectives:

- Explain the four access modes

- Describe the security appliance file management system

- Discuss security appliance security levels

- Configure a security appliance for basic network connectivity

- Use appropriate **show** commands to verify initial configuration

- Explain how to set the clock and synchronize the time on security appliances

- Configure the security appliance to send syslog messages to a syslog server

User Interface

This topic references access modes and commands associated with the operation of Cisco security appliances.

Security Appliance Access Modes

A Cisco security appliance has four administrative access modes:

- **Unprivileged** → `firewall>`
- **Privileged** → `firewall#`
- **Configuration** → `firewall<config>#`
- **Monitor** → `monitor>`

SNPA v4.0—3-3
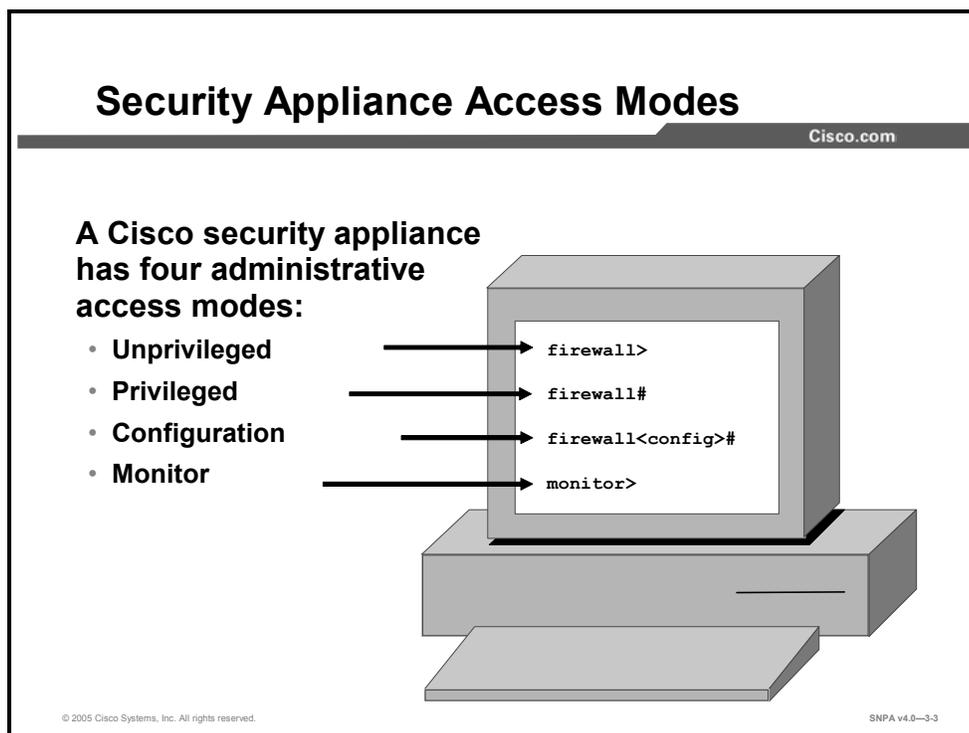
Cisco security appliances contain a command set based on Cisco IOS software, and they provide four administrative access modes:

- Unprivileged mode: Available when you first access the security appliance. The **>** prompt is displayed. This mode provides a restricted view of security appliance settings.

- Privileged mode: Displays the # prompt and enables you to change the current settings. Any unprivileged command also works in privileged mode.

- Configuration mode: Displays the (config)# prompt and enables you to change system configurations. All privileged, unprivileged, and configuration commands work in this mode.

- Monitor mode: A special mode that enables you to update the image over the network or to perform password recovery. While in the monitor mode, you can enter commands to specify the location of the Trivial File Transfer Protocol (TFTP) server and the location of the security appliance software image or password recovery binary file to download.

Within each access mode, you can abbreviate most commands down to the fewest unique characters for a command. For example, you can use **sh run** to view the configuration instead of the full command **show running-config**. You can use **en** instead of **enable** to start privileged mode, and **con t** instead of **configuration terminal** to start configuration mode.

Note   You can create your configuration on a text editor, then cut and paste it into the configuration. You can paste the configuration one line at a time or you can paste the entire configuration at once. Always check your configuration after pasting large blocks of text to be sure everything was copied correctly.

Access Privilege Mode

Internet
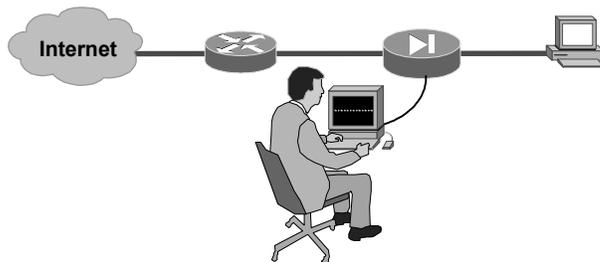
firewall>

```
enable [priv_level]
```

- **Used to control access to the privileged mode**
- **Enables you to enter other access modes**

```
pixfirewall> enable
password:
pixfirewall#
```

SNPA v4.0—3-4

Upon first accessing a security appliance, the administrator is presented with one of two prompts: **pixfirewall>** for a Cisco PIX 500 Series Security Appliance and **ciscoasa>** for a Cisco ASA 5500 Series Adaptive Security Appliance. This is the unprivileged mode. This mode enables you to view restricted settings. To get started with the security appliance, the first command you need to know is the **enable** command. It provides entrance to the privileged access modes. After you enter **enable**, the security appliance prompts you for your privileged mode password. By default, a password is not required, so you can press **Enter** at the password prompt or you can create a password of your choice. After you are in privileged mode, notice that the prompt has changed to #.

The **enable password** command sets the privileged mode password. The password is case-sensitive and can be up to 16 alphanumeric characters long. Any character except for the question mark, space, and colon can be used.

If you create a password, write it down and store it in a manner consistent with your site's security policy. After you create this password, you cannot view it again because it is stored as a Message Digest 5 (MD5) hash. The **show enable password** command lists the encrypted form of the password. After passwords are encrypted, they cannot be reversed to plain text.

The syntax for the **enable** commands is as follows:

```
enable
enable password pw [level priv_level] [encrypted]
```

priv_level	The privilege level, from 0 to 15.
pw	Specifies a case-sensitive password up to 16 alphanumeric characters.
encrypted	Specifies that the password you entered is already encrypted.

Note   An empty password is also changed into an encrypted string.

Access Configuration Mode: *configure terminal* Command

firewall#

```
configure terminal
```

- **Used to start configuration mode to enter configuration commands from a terminal**

firewall#

```
exit
```

- **Used to exit from an access mode**

```
pixfirewall> enable
password:
pixfirewall# configure terminal
pixfirewall(config)# exit
pixfirewall# exit
pixfirewall>
```

SNPA v4.0—3-5

Use the **configure terminal** command to move from privileged mode to configuration mode. As soon as you enter the command, the prompt changes to (config)#. Configuration mode enables you to change system configurations. Basic commands for security appliances are covered in greater detail later in this lesson. Use the **exit**, **end**, or **quit** command to exit and return to the previous mode.

help Command

```
pixfirewall > help ?

  enable  Turn on privileged commands
  exit    Exit the current command mode
  login   Log in as a particular user
  logout  Exit from current command mode, and to
           unprivileged mode
  quit    Exit the current command mode

pixfirewall > help enable

  USAGE:

        enable [<priv_level>]

  DESCRIPTION:

  enable          Turn on privileged commands
```

CSPFA v4.0—4-7

Help information is available via the security appliance command-line interface (CLI). If you specify **help** and enter **?**, for example, **pixfirewall> help ?**, then all commands that are available in the current privilege level and mode are displayed. In the figure, all the commands for unprivileged mode are displayed. You can see help, usage, description, and syntax for an individual command by entering the **help** command followed by the command name, for example, **pixfirewall> help enable**. In the figure, the usage and description for the **enable** command is displayed.

The syntax for the **help** command is as follows:

> help *command | ?*

command	Specifies the command about which you want information.
?	Displays all commands that are available in the current privilege level and mode.

If you do not know or are unsure of a command string, enter **?** after the command (for example, **enable ?**). The command syntax will be displayed, for example, **pixfirewall> enable ?**:

```
pixfirewall> enable ?
<0-15> Enter optional privilege level (0-15)
<cr>
```

File Management

This topic describes the file management system in the security appliance.

Viewing and Saving Your Configuration

Cisco.com

The following commands enable you to view or save your configuration:

- copy run start
  - show running-config
  - show startup-config
- write memory
  - write terminal

To save configuration changes:
copy run start

startup-config (saved) ← running-config ← Configuration Changes

SNPA v4.0—3-8

There are two configuration memories in the Cisco security appliances, running configuration and startup configuration. The **show running-config** command displays the current configuration in the security appliance's RAM on the terminal. Any changes made to the security appliance's configuration are written into the running configuration. This is volatile RAM. If the security appliance loses power or is rebooted, any changes to the running configuration that were not previously saved are lost. You can also display the current running configuration by using the **show running-config** command or the **write terminal** command.

The **copy run start** command and the **write memory** command save the current running configuration to Flash memory, startup configuration. It is the same as answering "yes" to the setup dialog prompt that asks if you wish to save the current configuration to Flash memory. When the configuration is written to Flash memory, you can view it by using either the **show startup-config** command or the **show configure** command.

Another useful command is **show history**, which displays previously entered commands. You can examine commands individually with the up and down arrows or by entering **Ctrl+P** to view previously entered lines and **Ctrl+N** to view the next line.

Clearing Running Configuration

Clear the running configuration:
clear config all

startup-config (default)   running-config
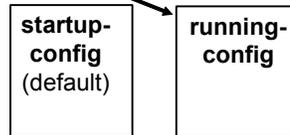
firewall(config)#

```
clear configure all
```

- **Clears the running-configuration**

```
fw1(config)# clear config all
```

SNPA v4.0—3-9

The **clear config all** command clears the running configuration. When you issue this command, the current running configuration is lost and is reset to the default running configuration. The startup configuration is not defaulted.

Clearing Startup Configuration

Clear the startup configuration:
Write erase

startup-config (default)

running-config

firewall#

```
write erase
```

• **Clears the startup configuration**

```
Fw1# write erase
```

The **write erase** command clears the startup configuration. When you issue this command, you are prompted to confirm if you want to erase the startup configuration. If you type "yes," the startup configuration is erased. At this point, you can power cycle or reboot the security appliance. The security appliance reverts to the default configuration. Or you can copy the running configuration to Flash by issuing the **copy run start** command.

Reload the Configuration: *reload* Command

firewall(config)#

```
reload [noconfirm] [cancel] [quick] [save-config]
[max-hold-time [hh:]mm [{in [hh:]mm |
{at hh:mm [{month day} | {day month}]}]}] [reason
text]
```

- **Reboots the security appliance and reloads the configuration**
- **Reboots can be scheduled**

```
fw1# reload
Proceed with reload?[confirm] y
Rebooting...
```

SNPA v4.0—3-11

The **reload** command enables you to reboot the security appliance. By default, the command is interactive. The security appliance first checks whether the configuration has been modified and not saved. If so, it prompts you to save the configuration. If you specify the **save-config** parameter, the configuration is saved without prompting. The security appliance then prompts you to confirm that you really want to reload the system. You are prompted for confirmation when the "Proceed with reload? [confirm]" message displays. Only a response of **y** or pressing **Enter** causes a reload. Upon confirmation, the security appliance starts or schedules the process, depending upon whether you have specified a delay parameter.

By default, the process operates in "graceful" (also known as "nice") mode. It notifies all registered subsystems that a reboot is about to occur, allowing these subsystems to shut down before the reboot. To avoid waiting until all such shutdowns occur, specify the **max-hold-time** parameter to specify a maximum time to wait. Alternatively, you can use the **quick** parameter to force the process to begin abruptly, without notifying the affected subsystems or waiting for a graceful shutdown.

You can force the **reload** command to operate noninteractively by specifying the **noconfirm** parameter. In this mode, **reload** does not check for an unsaved configuration unless you have specified the **save-config** parameter. It does not prompt the user for confirmation before rebooting the system. It starts or schedules the reload process immediately unless you have specified a delay parameter, although you can specify the **max-hold-time** or **quick** parameters to control the behavior or the reload process. Use the **reload cancel** command to cancel a scheduled reload. You cannot cancel a reload that is already in progress.

If you wish to return the security appliance back to a default configuration, use the **write erase** and **reload** commands. The **write erase** command clears the startup configuration and reverts it to default parameters. The **reload** command reboots the security appliance using the startup configuration, in this case the default configuration. An administrator can back up or restore a security appliance configuration.

File System

10.0.0.11

Release 6.
and earlier

- **Software Image**
- **Configuration file**
- **Private data file**
- **PDM image**
- **Crash information**

Release 7.
and later

- **Software image**
- **Configuration file**
- **Private data**
- **PDM image**
- **Backup image***
- **Backup configuration file***
- **Virtual firewall Configuration file***

* Space available
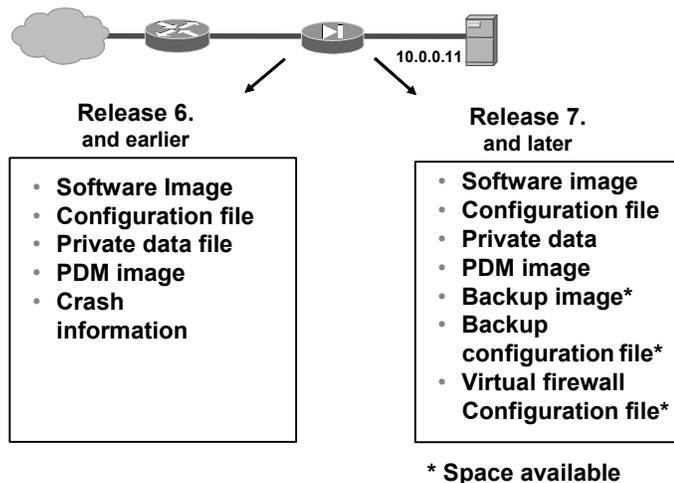
SNPA v4.0—3-12

In Cisco PIX Security Appliance Software v6.3 and earlier, the PIX Security Appliance file system supports a single version of the operating system image, the Cisco Pix Device Manager (PDM) image, and files. In Cisco PIX and ASA Security Appliance Software v7.0, the PIX 515E, 525, and 535 Security Appliances and the ASA Adaptive Security Appliance models support multiple images, configurations files, and syslog files. The number and size of the additional files is dependent on the amount of Flash memory in the security appliance. The PIX 515E, 525, and 535 security appliances ship with 16 MB of Flash, which may support only one software image and Cisco Adaptive Security Device Manager (ASDM) image and several configuration files. The ASA Security Appliance models with 64 MB of Flash may support multiple images and configuration files. The number of images and files is dependent on the amount of resident Flash on the specific security appliance.

Displaying Stored Files: System and Configuration
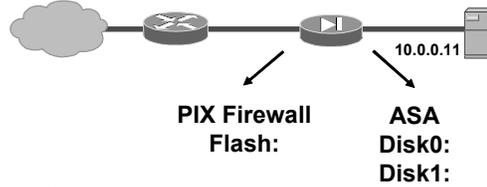
```
firewall(config)#
```

```
dir [/recursive]
[[{disk0:|disk1:|flash:}][<path>}]]
```

```
firewall# dir

Directory of flash:/

3     -rw-  4902912     13:37:33 Jul 27 2005  pix-701.bin
4     -rw-  6748932     13:21:13 Jul 28 2005  asdm-501.bin

16128000 bytes total (4472832 bytes free)
```

SNPA v4.0—3-13

To display the directory contents, use the **dir** command in privileged EXEC mode. The **dir** command without keywords or arguments displays the directory contents of the current directory. In the figure, asdm-501.bin and pix-701.bin software files are resident in flash. The command also displays the amount of free space available.

The syntax for the **dir** commands is as follows:

```
dir [/all] [all-filesystems] [/recursive] [disk0: | disk1: |
flash: | system:] [path]
```

all	Displays all files
All-filesystems	Displays the files of all file systems
Disk0:	Specifies the nonremovable, internal Flash memory DIMM, followed by a colon
Disk1:	Specifies the removable, external CompactFlash memory card, followed by a colon
/recursive	Displays the directory contents recursively
Flash:	Displays the directory contents of the default Flash partition
System:	Displays the directory contents of the file system
path	Specifies a specific path

If you want to view a configuration file stored in the directory, enter **more** plus the name of the configuration file.

Selecting Boot System File

```
firewall# dir

Directory of flash:/

3      -rw-  4902912    13:37:33 Jul 27 2005  pix-701.bin
4      -rw-  6748932    13:21:13 Jul 28 2005  asdm-501.bin

16128000 bytes total (4472832 bytes free)
```

```
firewall(config)#
```

```
Boot [system | config} <url>
```

- **Can store more than one system image and configuration file**
- **Designates which system image and startup configuration file to boot**

```
fw1(config)# boot system flash:/pix-701.bin
```

SNPA v4.0—3-14

To specify which system image the system will use at next reload and which configuration file the system will use at startup, use the **boot** command in privileged EXEC mode. For the **boot system** command, there are no defaults. Upon reload or a power cycle, if the boot environment variable is not configured, the system will boot the first valid image found in the internal flash. If no valid image is found, no system image will be loaded, and the system will boot loop until ROMMON or Monitor mode is broken into, **Escape** for the PIX Security Appliance and **Ctrl+R** for the ASA Security Appliance.

You can enter up to four **boot system** commands, to specify different images from which to boot in order, and the security appliance will boot the first valid image it finds.

Use the **no** form of this command to restore the default value.

The syntax for the **boot** commands is as follows:

```
boot {config |system} url
```

config	Specifies which configuration file to use when the system is loaded.
system	Specifies which system image file to use when the system is loaded.

url	Sets the context configuration URL. All remote URLs must be accessible from the admin context. See following URL syntax:
	• disk0:/*[path/]filename*
	This option is only available for the ASA platform and indicates the internal Flash card. You can also use Flash instead of disk0; they are aliased.
	• disk1:/*[path/]filename*
	This option is only available for the ASA platform and indicates the external Flash card.
	• flash:/*[path/]filename*
	• tftp://*[user[:password*]@]*server[:port]/[path/]filenam*e

Verifying the Startup System Image

Cisco.com

10.0.0.11

Boot Image
flash:/pix-701.bin
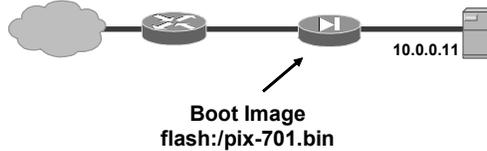
firewall(config)#

```
show bootvar
```

```
fw1# show bootvar

BOOT variable = flash:/pix-701.bin          Running
Current BOOT variable = flash:/pix-701.bin  Configured
CONFIG_FILE variable =
Current CONFIG_FILE variable =
```

SNPA v4.0—3-15

To show the configured and running boot files, use the **show boot** command in privileged mode. In the figure, Current BOOT variable is the configured boot variable, flash:/pix-701.bin. The flash:/pix-701.bin image file is booted when the system reloads or is power cycled. The boot variable, flash:/pix-701.bin, is the currently running version of the operating software.

```
fw1# show bootvar

BOOT variable = flash:/pix-701.bin
Current BOOT variable = <blank>
CONFIG_FILE variable =
Current CONFIG_FILE variable =
```

Upon reload or a power cycle, if Current BOOT variable is not configured, the system will boot the first valid image that it finds in the internal Flash.

Security Appliance Security Levels

This topic discusses the security levels of the Cisco security appliances.

Functions of the Security Appliance: Security Algorithm

- **Implements stateful connection control through the security appliance.**
- **Allows one-way (outbound) connections with a minimum number of configuration changes. An outbound connection is a connection originating from a host on a more-protected interface and destined for a host on a less-protected network.**
- **Monitors return packets to ensure that they are valid.**
- **Randomizes the first TCP sequence number to minimize the risk of attack.**

The security appliance security algorithm is a stateful approach to security. Every inbound packet (the packet originating from a host on a less-protected network and destined for a host on a more-protected network) is checked against connection state information in the security appliance's memory. Knowledge of the security algorithm is fundamental to implementing Internet access security because it performs the following tasks:

- Implements stateful connection control through the security appliance.

- Allows one-way (outbound) connections with a minimum number of configuration changes. An outbound connection is a connection originating from a host on a more-protected interface and destined for a host on a less-protected network.

- Monitors return packets to ensure that they are valid.

- Randomizes the first TCP sequence number to minimize the risk of attack.

The security algorithm maintains the secure perimeters between the networks controlled by the security appliance. The stateful connection-oriented security algorithm design creates session flows based on source destination addresses as well as TCP and User Datagram Protocol (UDP) port numbers. The security algorithm randomizes TCP sequence numbers before the completion of the connection. This function is always running, monitoring return packets to ensure that they are valid.

Security Level Example

Cisco.com

DMZ Network

Ethernet2
• Security level **50**
• Interface name = DMZ

e2

Internet

e0 — **e1**

Outside Network

Ethernet0
• Security level **0**
• Interface name = outside

Inside Network

Ethernet1
• Security level **100**
• Interface name = inside
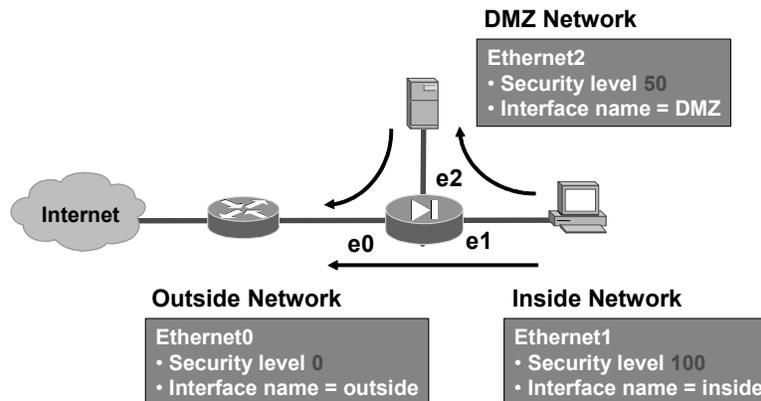
SNPA v4.0—3-18

The security level designates whether an interface is trusted (and more protected) or untrusted (and less protected) relative to another interface. An interface is considered trusted (and more protected) in relation to another interface if its security level is higher than the other interface's security level. An interface is considered untrusted (and less protected) in relation to another interface if its security level is lower than the other interface's security level.

The primary rule for security levels is that an interface with a higher security level can access an interface with a lower security level. Conversely, an interface with a lower security level cannot access an interface with a higher security level without an access control list (ACL), which is discussed later in the lesson. Security levels range from 0 to 100:

■ Security level 100: This is the highest security level for the inside interface of the security appliance. This is the default setting for the security appliance and cannot be changed. Because 100 is the most trusted interface security level, your corporate network should be set up behind it. This is so that no one else can access it unless they are specifically given permission and so that every device behind this interface can have access outside the corporate network.

■ Security level 0: This is the lowest security level for the outside interface of the security appliance. This is the default setting for the security appliance and cannot be changed. Because 0 is the least-trusted interface security level, you should set your most untrusted network behind this interface so that it does not have access to other interfaces unless it is specifically given permission. This interface is usually used for your Internet connection.

■ Security levels 1–99: These are the security levels that you can assign to the perimeter interfaces connected to the security appliance. You assign the security levels based on the type of access you want each device to have.

The following are examples of different interface connections between the security appliance and other perimeter devices:

■ More secure interface (the higher security level) to a less secure interface (the lower security level): Traffic originating from the inside interface of the security appliance with a security level of 100 to the outside interface of the security appliance with a security level of 0 follows this rule: Allow all IP-based traffic unless restricted by ACLs, authentication, or authorization.

■ Less secure interface (lower security level) to a more secure interface (higher security level): Traffic originating from the outside interface of the security appliance with a security level of 0 to the inside interface of the security appliance with a security level of 100 follows this rule: Drop all packets unless specifically allowed by an **access list** command. Further restrict the traffic if authentication and authorization is used.

■ Same secure interface to a same secure interface: No traffic flows between two interfaces with the same security level.

This table explains the diagram in the previous figure.

Security Levels

Interface Pair	Relative Interface Relationship for Ethernet2 (DMZ) Interface	Configuration Guidelines
Outside security 0 to demilitarized zone (DMZ) security 50	DMZ is considered trusted.	Statics and ACLs must be configured to enable sessions originated from the outside interface to the DMZ interface.
Inside security 100 to DMZ security 50	DMZ is considered untrusted.	Globals and Network Address Translation (NAT) are configured to enable sessions that originate from the inside interface to the DMZ interface. Statics may be configured for the DMZ interface to ensure that service hosts have the same source address.

Note   The security appliance can support up to 14 interfaces, depending on the model and license.

Basic Security Appliance Configuration

This topic contains the basic commands that make the security appliance operational.

The following are some of the primary configuration commands for the security appliance.

- **hostname**: Assigns a hostname to the security appliance

- **interface**: Configures the type and capability of each perimeter interface

    — **nameif**: Assigns a name to each perimeter interface

    — **ip address**: Assigns an IP address to each interface

    — **security level**: Assigns the security level for the perimeter interface

    — **speed**: Assigns the connection speed

    — **duplex**: Assigns the duplex communications

    — **no shutdown**: Enables the interface

- **nat-control**: Enable or disable NAT configuration requirement

- **nat**: Shields IP addresses on the inside network from the outside network

- **global**: Creates a pool of one or more IP addresses for use in NAT and port address translation (PAT)

- **route**: Defines a static or default route for an interface

Assigning Hostname to Security Appliance: Changing the CLI Prompt

New_York
Server

Boston
Server

Dallas
Server
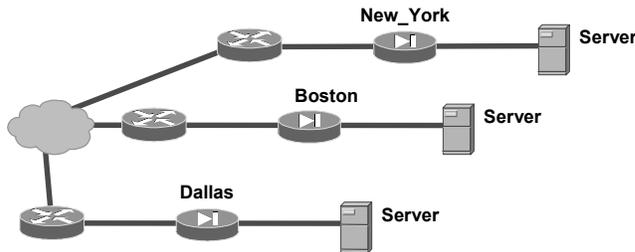
pixfirewall(config)#

```
hostname newname
```

- **Changes the hostname in the PIX Firewall CLI prompt**

```
pixfirewall(config)# hostname Boston
Boston(config)#
```

SNPA v4.0—3-20

In the example in this figure, notice that the default hostname label for the security appliance is **pixfirewall**. This default hostname is for PIX Security Appliances. The default hostname for the ASA Adaptive Security Appliances is **ciscoasa**. In a network of multiple security appliances, it may be advantageous to assign a unique hostname label to each security appliance. To accomplish this, use the **hostname** command. The **hostname** command changes the hostname label on the prompts. The hostname can be up to 63 alphanumeric characters and uppercase and lowercase. The figure shows the default hostname label of **pixfirewall** being changed to **Boston**.

The syntax for the **hostname** command is as follows:

```
hostname newname
```

newname	New hostname for the security appliance prompt

interface Command and Sub-commands

Cisco.com

ethernet2

e2

Internet

e0   e1

ethernet0   ethernet1
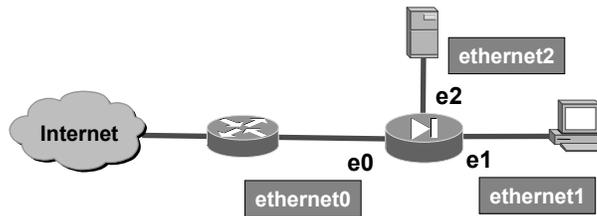
pixfirewall(config)#

```
interface hardware_id
```

• **Specifies a perimeter interface and its slot location on the firewall.**

```
pix1(config)# interface ethernet0 (GigabitEthernet0/0)
pix1(config-if)#
```

CSPFA v4.0—4-23

The **interface** command identifies a perimeter interface and its slot location on the security appliance. The PIX Security Appliance interfaces are numbered from 0 to X (X = highest-numbered interface on the PIX Security Appliance). The ASA Adaptive Security Appliance interfaces are numbered 0/0, 0/1, 0/2, and so on. For each security appliance in your network, enter the appropriate interface type and slot and port number. In the figure, if the device is a PIX Security Appliance, enter interface Ethernet0. If the device is an ASA Security Appliance, enter either GigabitEthernet0/0 or Management0/0 for the management interface. After entering the **interface** command, the CLI prompt changes to the interface configuration subcommand level. With interface configuration subcommands, you can configure hardware speed and duplex, assign a name, assign a security level, assign an IP address, and configure many other settings. For an interface to pass traffic, you must configure these subcommands: **nameif**, **ip address**, **security-level**, and **no shutdown**. For physical interfaces, the default state is to be shut down; use the **no shutdown** command to change the default. You must also verify the security level for the interface by accepting the default or changing from the default level so that interfaces can communicate with each other. Interface configuration subcommands are covered in greater detail later in this lesson.

The syntax for the **interface** command is as follows:

```
interface {physical_interface[.subinterface] | mapped_name}
```

mapped_name	In multiple context mode, enter the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	Enter the physical interface type, slot, and port number as *type*[*slot*/]*port*. A space between the type and slot/port is optional. Depending on your security appliance model, interface types include the following: • **ethernet** • **gigabitethernet** • **management** If your model does not include slots, then enter the interface type followed by the port number. If your model includes slots, then enter the interface type followed by *slot*/*port*. See the hardware documentation that came with your model to identify the interface type, slot, and port number.
subinterface	(Optional) Enter an integer between 1 and 4294967293 to designate a logical subinterface.

Assign an Interface Name:
nameif **Subcommand**

Ethernet2
• Interface name = dmz

Internet

e2

e0 e1

Ethernet0
• Interface name = outside

Ethernet1
• Interface name = inside
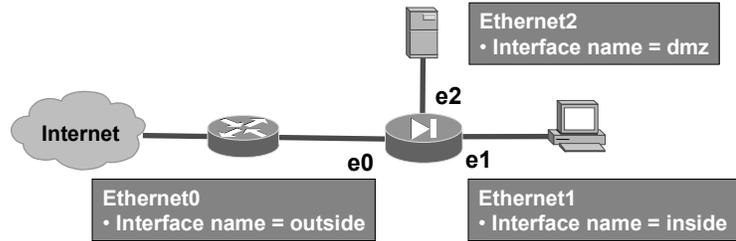
firewall(config-if)#

```
nameif hardware_id if_name
```

• **Assigns a name to each perimeter interface on the PIX Firewall Security Appliance.**

```
fw1(config)# interface ethernet0 (GigabitEthernet0/0)
fw1(config-if)# nameif outside
```

SNPA v4.0—3-23

The subcommand **nameif** assigns a name to each interface on the security appliance. The first two interfaces have the default names **inside** and **outside**. In the figure, interface Ethernet2 is assigned the name **dmz**.

The syntax for the **nameif** command is as follows:

```
nameif hardware_id if_name
```

hardware_id	The hardware name for the network interface that specifies the slot location of the interface on the security appliance motherboard. For more information on security appliance hardware configuration, refer to the *Cisco Security appliance Hardware Installation Guid*e.
	A logical choice for an Ethernet interface is **ethernet*n*.** These names can also be abbreviated with any leading characters in the name, for example, **ether1** or **e2**.
if_name	Describes the perimeter interface. This name is assigned by you, and must be used in all future configuration references to the perimeter interface.

Assign Interface IP Address—
ip address Sub-command

Cisco.com
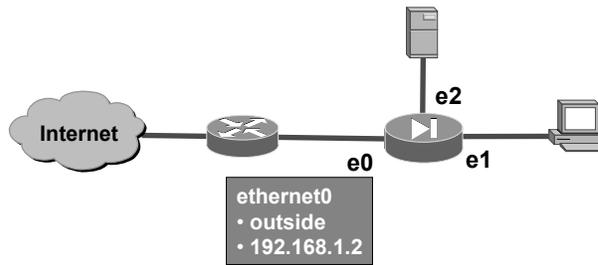
pixfirewall(config-if)#

```
ip address ip_address [netmask]
```

• **Assigns an IP address to each interface.**

```
pix1(config)# interface ethernet0 (GigabitEthernet0/0)
pix1(config-if)# nameif outside
pix1(config-if)# ip address 192.168.1.2 255.255.255.0
```

CSPFA v4.0—4-25

Each interface on the security appliance can be configured with an IP address. Use the **ip address** interface configuration subcommand for this purpose. If you make a mistake while entering this command, reenter it with the correct information. The **clear configure ip** command resets all interface IP addresses to no IP address. In the figure, the dmz interface is configured with an IP address of 172.16.0.1 and a mask of 255.255.255.0. This command also sets the standby address for failover.

The syntax for the **ip address** command is as follows:

```
ip address ip_address [mask] [standby ip_address]
```

ip_address	Specifies the IP address of the interface.
mask	(Optional) The subnet mask for the IP address. If you do not set the mask, the security appliance uses the default mask for the IP address class.
standby ip_address	(Optional) The IP address for the standby unit for failover.

DHCP-Assigned Address

Cisco.com

DHCP Assigned

Internet

e0

Ethernet0
• **Interface name = outside**
• **IP address = DHCP**
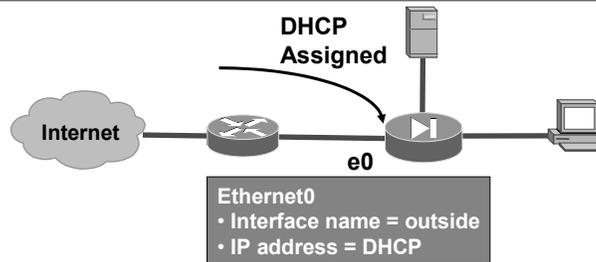
firewall(config-if)#

```
ip address if_name dhcp [setroute] [retry
retry_cnt]
```

• **Enables the DHCP client feature on the outside interface**

```
fw1(config)# interface ethernet0 (GigabitEthernet0/0)
fw1(config-if)# nameif outside
fw1(config-if)# ip address dhcp
```

SNPA v4.0—3-25

Instead of manually configuring an IP address on the security appliance's interface, you can enable the security appliance's Dynamic Host Configuration Protocol (DHCP) client feature to have the security appliance dynamically retrieve an IP address from a DHCP server. With the security appliance configured as a DHCP client, a DHCP server can configure the security appliance's interface with an IP address, subnet mask, and (optional) a default route. Use the **ip address dhcp** subcommand to enable this feature. In the figure, the security appliance is configured to receive an IP address on the outside interface via DHCP.

Also, use the **ip address dhcp** subcommand to release and renew a DHCP lease from the security appliance. To delete the DHCP leased IP address, use the subcommand **no ip address dhcp**. The **debug dhcpc event | packet | error** command provides debugging tools for the DHCP client feature.

The syntax for the **ip address dhcp** subcommand is as follows:

```
ip address dhcp [setroute] [retry retry_cnt]
show ip address if_interface dhcp lease | server
no ip address dhcp
```

dhcp	Specifies that the security appliance will use DHCP to obtain an IP address.

setroute	Tells the security appliance to set the default route using the default gateway parameter that the DHCP server returns.
retry	Enables the security appliance to retry a poll for DHCP information.
retry_cnt	Specifies the number of times the security appliance will poll for DHCP information. The values available are 4 to 16. The default is 4.

Use the **show ip address** *if_interface* **dhcp lease** command to view current information about your DHCP lease. Use the **show ip address** *if_interface* **dhcp server** command to view current information about your DHCP server.

The following is an example of dhcp lease and server statistics available on a security appliance:

```
pix1# show ip address outside dhcp lease

Temp IP addr: 192.168.1.3  for peer on Interface: outside
Temp  sub net mask: 255.255.255.0
   DHCP Lease server: 172.26.26.50, state: 3 Bound
   DHCP transaction id: 0x902F
   Lease: 691200 secs, Renewal: 345600 secs,  Rebind: 604800
secs
   Next timer fires after: 345593 seconds
   Retry count: 0 Client-ID: cisco-000b.fcf8.c538-outside-3
   Proxy: FALSE
   Hostname: pix1

pix1(config-if)# show ip address outside dhcp server

   DHCP server: ANY (255.255.255.255)
    Leases:   0
    Offers:   0      Requests: 0      Acks: 0      Naks: 0
    Declines: 0      Releases: 0      Bad:  0

   DHCP server: 172.26.26.50
    Leases:   1
    Offers:   1      Requests: 1      Acks: 1      Naks: 0
    Declines: 0      Releases: 0      Bad:  0
    Subnet: 255.255.255.0
```

Note   A security appliance that is configured as a DHCP client does not support failover configurations.

Assign an Security-Level —*security-level* Sub-commands
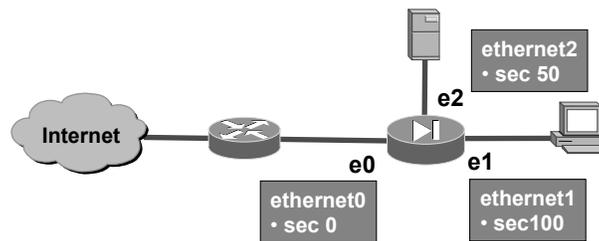
pixfirewall(config-if)#

```
security-level [level]
```

- **Assigns a security level to the interface.**

```
pix1(config)# interface ethernet0 (GigabitEthernet0/0)
pix1(config-if)# nameif outside
pix1(config-if)# ip address 192.168.1.2
pix1(config-if)# security-level 0
```

CSPFA v4.0—4-27

The **security-level** interface configuration subcommand specifies the security appliance security level (except for the inside and outside security appliance interfaces, which are assigned security levels by default). The inside interface has a default security level of 100; the outside interface has a default security level of 0. As other interfaces are named, the system assigns a default security level of 0 to each interface. For these newly named interfaces, the administrator should change the system-assigned default security level to a unique number from 1 through 99.

The syntax for the **security-level** command is as follows:

```
security-level number
```

number	An integer between 0 (lowest) and 100 (highest)

Normally, interfaces on the same security level cannot communicate. If you want interfaces on the same security level to communicate, use the **same-security-traffic** command. You might want to assign two interfaces to the same level and allow them to communicate if you do not want to perform NAT, if you want to create more than 101 communicating interfaces, and if you want protection features to be applied equally for traffic between two interfaces (for example, if you have two departments that are equally secure).

If you change the security level of an interface and you do not want to wait for existing connections to time out before the new security information is used, you can clear the translation table using the **clear xlate** command. However, clearing the translation table disconnects all current connections.

Assign an Interface Speed and Duplex: *speed* and *duplex* SubCommands

Cisco.com
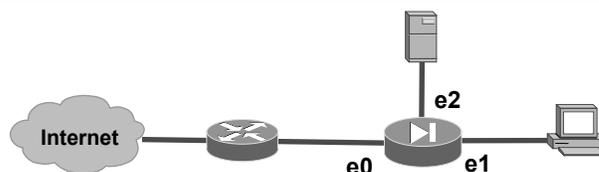
Ethernet0
- Speed =100
- Duplex = full

firewall(config-if)#

```
speed [hardware_speed]
duplex [duplex_operation]
```

- **Enables an interface speed and duplex**

```
fw1(config)# interface ethernet0 (GigabitEthernet0/0)
fw1(config-if)# nameif outside
fw1(config-if)# ip address 192.168.1.2
fw1(config-if)# security-level 0
fw1(config-if)# speed 100
fw1(config-if)# duplex full
```

SNPA v4.0—3-27

The hardware speed is set to automatic speed sensing by default; it is recommended that you specify the speed of the network interfaces. This enables the security appliance to operate in network environments that may include switches or other devices that do not handle automatic sensing correctly.

To set the speed of a copper (RJ-45) Ethernet interface, use the **speed** interface configuration subcommand. To restore the speed setting to the default, use the **no** form of this command.

The syntax for the **speed** command is as follows:

```
speed {auto | 10 | 100 | nonegotiate}
```

10	Sets the speed to 10BASE-T.
100	Sets the speed to 100BASE-T.
auto	Automatically detects the speed.
nonegotiate	For a small-form-factor pluggable (SFP) media type, sets the speed to 1000 Mbps. SFP does not allow any other setting.

To set the duplex of RJ-45 Ethernet interfaces, use the **duplex** interface configuration subcommand. To restore the duplex setting to the default, use the **no** form of this command.

The syntax for the **duplex** command is as follows:

```
duplex {auto | full | half}
```

auto	Automatically detects the duplex mode
full	Sets the duplex mode to full duplex
half	Sets the duplex mode to half duplex

ASA Management Interface

Internet

e2

e0   **e1**

Ethernet0
• Management = only
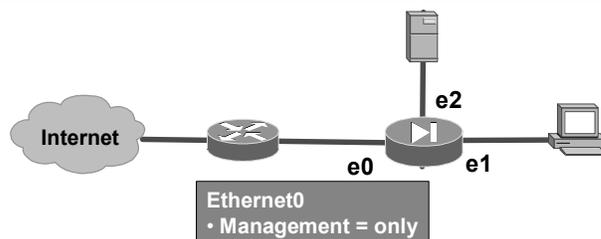
firewall(config-if)#

```
management-only
no management-only
```

• **To set an interface to accept management traffic only**

```
fw1(config)# interface management 0/0
fw1(config-if)# nameif outside
fw1(config-if)# ip address 192.168.1.2
fw1(config-if)# security-level 0
```

SNPA v4.0—3-28

To set an interface to accept management traffic only, use the **management-only** interface configuration subcommand. You can configure any interface to be a management-only interface using the **management-only** command. To allow through-traffic, use the **no** form of this command.

The ASA Adaptive Security Appliance includes a dedicated management interface called Management 0/0, which is meant to support management traffic to the security appliance only. To disable management-only mode so that the interface can allow through-traffic, enter the **no management-only** command (ASA 5520 or 5540 only).

Network Address Translation

NAT

192.168.0.20   10.0.0.11

Internet

192.168.10 .11   10.0.0.11

10.0.0.4

Translation Table	Outside Mapped Pool	Inside Local
	192.168.0.20	10.0.0.11
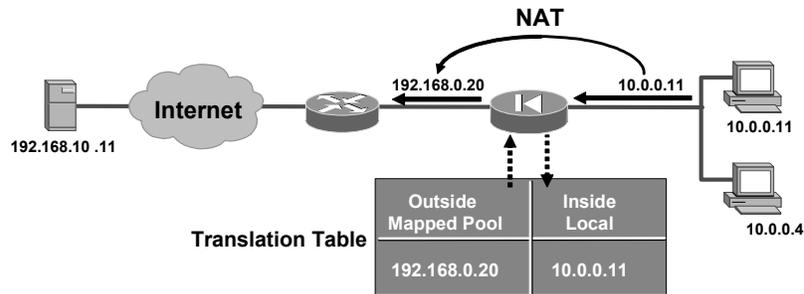
     SNPA v4.0—3-29

NAT enables you to prevent external networks from learning your internal IP addresses, those behind the security appliance. NAT accomplishes this by translating the internal IP addresses, which are not globally unique, into globally accepted IP addresses before packets are forwarded to the external network. NAT is implemented in the security appliance with the **nat** and **global** commands.

When an outbound IP packet that is sent from a device on the inside network reaches a security appliance that has NAT configured, the source address is extracted and compared with an internal table of existing translations. If the device's address is not already in the table, it is then translated. A new entry is created for that device, and it is assigned an IP address from a pool of mapped IP addresses. This mapped pool is configured using the **global** command. After this translation occurs, the table is updated and the translated IP packet is forwarded. After a user-configurable timeout period (or the default of three hours), during which there have been no translated packets for that particular IP address, the entry is removed from the table, and the mapped address is freed for use by another inside device.

In the figure, host 10.0.0.11 starts an outbound connection. The security appliance translates the source address to 192.168.0.20. Packets from host 10.0.0.11 are seen on the outside as having a source address of 192.168.0.20. Return packets from the outside server at IP address 192.168.10.11 are addressed to the mapped address, 192.168.0.20.

Enable NAT Control

NAT

192.168.0.20   10.0.0.11

Internet

200.200.200.11

10.0.0.11

10.0.0.4

Translation Table

Outside Mapped Pool	Inside Local
192.168.0.20	10.0.0.11
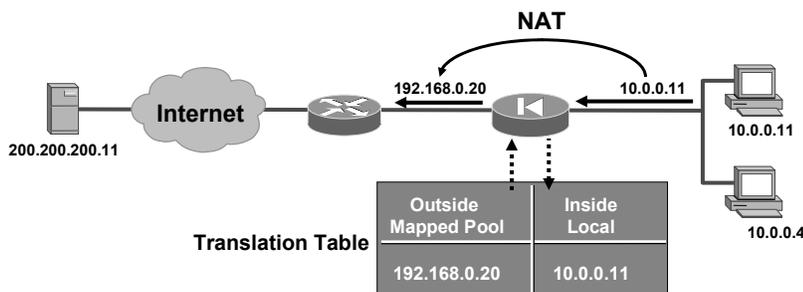
• **Enable or disable NAT configuration requirement**

```
fw1(config)# nat-control
```

SNPA v4.0—3-30

The **nat-control** command enables NAT to be enabled incrementally. With **nat-control** disabled, only IP addresses that need to be protected require a NAT rule. With **nat-control** enabled, all packets traversing the security appliance require a NAT rule. There are two NAT policies, an inside NAT policy and an outside NAT policy. They are used to perform address translation on each packet that traverses the security appliance. If NAT control is configured, the security appliance enforces address hiding. Specifically, each inside address must have an inside NAT rule configured before communication is permitted through the security appliance. If outside NAT is enabled on an interface, each outside address must have an outside NAT rule configured before communication is permitted through the security appliance. If **no nat-control** is configured, only hosts that undergo NAT need a NAT rule configured. If there is no NAT policy that matches the traversing packet, address rewrite is not performed and security appliance processing continues. No NAT control is the default.

nat Command

Cisco.com
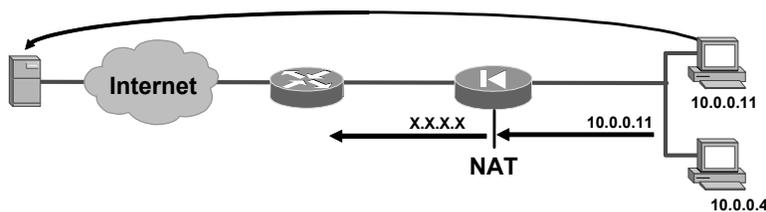
```
firewall(config)#
```

```
nat [(if_name)] nat_id address [netmask] [dns]
  [[tcp] tcp_max_conns [emb_limit]
  [norandomseq]]] [udp udp_max_conns]
```

• **Enables IP address translation**

```
fw1(config)# nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

The first step in enabling NAT on a security appliance is entering the **nat** command. The **nat** command can specify translation for a single host or a range of hosts. The **nat** command has two major components, *nat_id* and an IP address or range of IP addresses. *nat_id* is a number from 1 to 2147483647 that specifies the hosts for dynamic address translation. The dynamic addresses are chosen from a mapped address pool that is created with the **global** command. The **nat** command *nat_id* number must match the *nat_id* number in the **global** command if you want to use that specific mapped pool of IP addresses for the dynamic address translation.

For example, the **nat (inside) 1 10.0.0.0 255.255.255.0** command means that all outbound connections from a host within the specified network, 10.0.0.0, can pass through the security appliance (with address translation). The **nat (inside) 1 10.0.0.11 255.255.255.255** command means that only outbound connections originating from the inside host 10.0.0.11 are translated as the packet passes through the security appliance. Use **0.0.0.0** to allow all hosts to be translated. The **0.0.0.0** can be abbreviated as **0**. As shown in the example, all inside hosts making outbound connections with the **nat (inside) 1 0.0.0.0 0.0.0.0** command are translated. The *nat_id* identifies the mapped address pool that the security appliance will use for the dynamic address translation.

The syntax for the **nat** command is as follows:

```
nat [(if_name)] nat_id address [netmask] [dns] [[tcp]
    tcp_max_conns [emb_limit] [norandomseq]]] [udp udp_max_conns]
```

if_name	The name of the interface attached to the network to be translated.
nat_id	A number greater than zero (0) that specifies the mapped address pool that you want to use for dynamic address translation.
address	The IP address to be translated. You can use **0.0.0.0** to allow all hosts to start outbound connections. The **0.0.0.0** can be abbreviated as **0**.
netmask	Network mask for the address. You can use **0.0.0.0** to allow all outbound connections to translate with IP addresses from the mapped pool.
dns	Specifies to use the created translation to rewrite the Domain Name System (DNS) address record.
max_conns	The maximum number of simultaneous connections that the local IP hosts are to allow. (Idle connections are closed after the idle timeout specified by the **timeout conn** command.)
emb_limit	The maximum number of embryonic connections per host. (An embryonic connection is a connection request that has not finished the necessary handshake between source and destination.) Set a lower value for slower systems and a higher value for faster systems. The default is 0, which allows unlimited embryonic connections.
tcp	(Optional) Specifies that the maximum TCP connections and embryonic limit are set for the TCP protocol.
tcp_max_conns	(Optional) Maximum number of simultaneous TCP connections that the local IP hosts allow. (Idle connections are closed after the time that is specified by the **timeout conn** command.)
udp	(Optional) Specifies a maximum number of UDP connection parameters that can be configured.
udp_max_conns	(Optional) Sets the maximum number of simultaneous UDP connections that the local IP hosts are each allowed to use. (Idle connections are closed after the time that is specified by the **timeout conn** command.)

global **Command**

Cisco.com

Internet 192.168.0.20 10.0.0.11 10.0.0.11

NAT 10.0.0.4
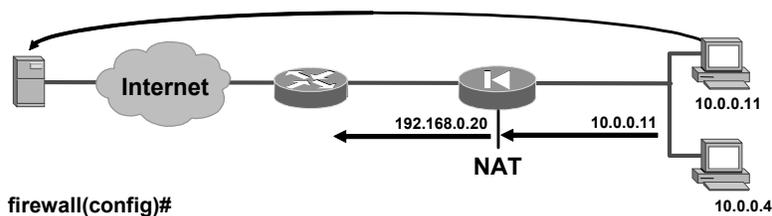
firewall(config)#

```
global[(if_name)] nat_id {mapped_ip[-mapped_ip]
   [netmask mapped_mask]} | interface
```

• **Works with the** nat **command to assign a registered or public IP address to an internal host when accessing the outside network through the firewall, for example, 192.168.0.20-192.168.0.254**

```
fw1(config)# nat (inside) 1 0.0.0.0 0.0.0.0
fw1(config)# global (outside) 1 192.168.0.20-192.168.0.254
```

SNPA v4.0—3-32

When an outbound IP packet that is sent from any device on the inside network reaches a security appliance that has NAT configured, the source address is extracted and compared with an internal table of existing translations. If the device's address is not already in the translation table, it is then translated. It is assigned an IP address from a pool of mapped IP addresses. In a security appliance configuration, there may be more than one mapped pool configured. Each outbound NAT is associated with a NAT identifier (NAT ID). Each mapped pool has a corresponding NAT ID. The security appliance uses the NAT ID of the outbound IP packet to identify which mapped pool of addresses to select a translation IP address from. The NAT ID of the outbound packet must match the NAT ID of the mapped pool. The security appliance assigns addresses from the designated mapped pool starting from the low end and going to the high end of the range that was specified in the **global** command. The pool of mapped IP addresses is configured with the **global** command.

In the figure, host 10.0.0.11 starts an outbound connection. The NAT ID of the outbound packet is 1. In this instance, a mapped IP address pool of 192.168.0.20-254 is also identified with a NAT ID of 1. The security appliance assigns an IP address of 192.168.0.20. It is the lowest available IP address of the range specified in the **global** command. Packets from host 10.0.0.11 are seen on the outside as having a source address of 192.168.0.20.

The syntax for the **global** command is as follows:

```
global [(if_name)] nat_id {mapped_ip [-mapped_ip] [netmask
mapped_mask]} | interface
```

if_name	Describes the external network interface name where you will use the mapped addresses.
nat_id	Identifies the mapped pool and matches it with its respective **nat** command.
mapped_ip	Single IP addresses or the beginning IP address for a range of mapped IP addresses.
mapped_ip	A range of mapped IP addresses.
mapped_mask	The network mask for the *mapped_ip* address. If subnetting is in effect, use the subnet mask (for example, 255.255.255.128). If you specify an address range that overlaps subnets with the **netmask** command, this command will not use the broadcast or network address in the pool of mapped addresses. For example, if you use 255.255.255.128 and an address range of 192.150.50.20–192.150.50.140, the 192.150.50.127 broadcast address and the 192.150.50.128 network address will not be included in the pool of mapped addresses.
interface	Specifies PAT using the IP address at the interface.

If the **nat** command is used, the companion command, **global**, must be configured to define the pool of translated IP addresses.

Use the **no global** command to delete a global entry (for example, **no global (outside) 1 192.168.1.20–192.168.1.254 netmask 255.255.255.0**).

Note	The security appliance uses the mapped addresses to assign a virtual IP address to an internal NAT address. After adding, changing, or removing a global statement, use the **clear xlate** command to make the IP addresses available in the translation table.

Configure a Static Route: *route* Command

Cisco.com

Default Route   **Static Route**

Internet

192.168.0.1   10.0.0.102

10.0.1.11

10.0.1.4
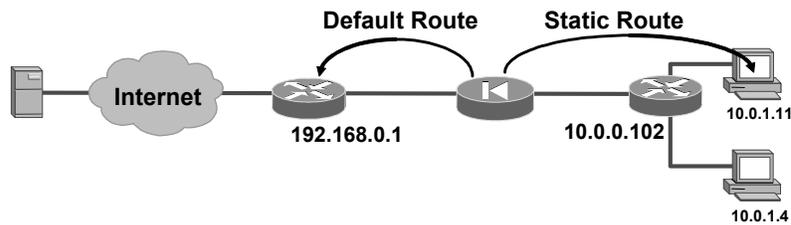
firewall(config)#

```
route if_name ip_address netmask gateway_ip
  [metric]
```

- **Defines a static or default route for an interface**

```
fw1(config)# route outside 0.0.0.0 0.0.0.0 192.168.0.1 1
fw1(config)# route inside 10.0.1.0 255.255.255.0 10.0.0.102 1
```

SNPA v4.0—3-33

Use the **route** command to enter a static route for an interface. To enter a default route, set *ip_address* and *netmask* to **0.0.0.0** (or the shortened form, **0**). In the figure, a **route** command with the IP address of 0.0.0.0 identifies the command as the default route. The security appliance transmits all destination packets not listed in its routing table from the outside interface to the router at IP address 192.168.0.1.

Create static routes to access specific networks beyond the locally connected networks. A static route is, in essence, stating, "To send a packet to the specified network, give it to this router." For example, in the figure, the security appliance sends all packets destined to the 10.0.1.0 255.255.255.0 network from the inside interface to the router at IP address 10.0.0.102. This was accomplished by using the following static **route** command: **route inside 10.0.1.0 255.255.255.0 10.0.0.102 1.** The router knows how to route the packet to the destination network of 10.0.1.0.

The syntax for the **route** command is as follows:

```
route if_name ip_address netmask gateway_ip [metric]
```

if_name	Describes the internal or external network interface name.
ip_address	Describes the internal or external network IP address. Use **0.0.0.0** to specify a default route. The 0.0.0.0 IP address can be abbreviated as 0.
netmask	Specifies a network mask to apply to the IP address. Use **0.0.0.0** to specify a default route. The 0.0.0.0 netmask can be abbreviated as 0.
gateway_ip	Specifies the IP address of the gateway router (the next hop address for this route).
metric	Specifies the number of hops to the gateway IP. If you are not sure, enter **1**. Your WAN administrator can supply this information or you can use a **traceroute** command to obtain the number of hops. The default is 1 if a metric is not specified.

You can use the IP address of one of the security appliance's interfaces as the gateway address. If this is done, the security appliance broadcasts an Address Resolution Protocol (ARP) request for the MAC address of the destination IP address in the packet instead of broadcasting a request for the MAC address of the gateway IP address.

HostName-to-IP-Address Mapping: *name* Command

"bastionhost"
172.16.0.2

172.16.0.0

.2

.1

10.0.0.0

"insidehost"
10.0.0.11

.1   .11
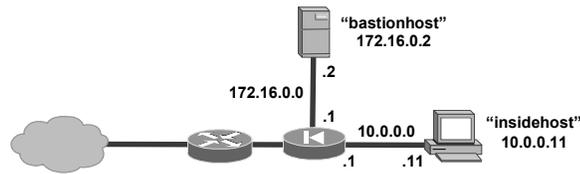
```
firewall(config)#

name ip_address name
```

- **Configures a list of name-to-IP-address mappings on the security appliance**

```
fw1(config)# names
fw1(config)# name 172.16.0.2 bastionhost
fw1(config)# name 10.0.0.11 insidehost
```

SNPA v4.0—3-34

The use of the **name** command enables you to configure a list of name-to-IP-address mappings on the security appliance. This allows the use of names in the configuration instead of IP addresses. In the figure, the server's and the PC's IP addresses are mapped to names, bastionhost and insidehost. Bastionhost and insidehost can be used in place of an IP address in any security appliance command reference, for instance, the command **ping insidehost**.

The syntax for the **name** command is as follows:

```
name ip_address name
```

ip_address	The IP address of the host being named
name	The name assigned to the IP address

Allowable characters for the name are: a through z, A through Z, 0 through 9, a dash (-), and an underscore (_). The name cannot start with a number. If the name is more than 16 characters long, the **name** command fails. After the name is defined, it can be used in any security appliance command reference in place of an IP address. The **names** command enables the use of the **name** command. The **clear configure names** command clears the list of names from the security appliance configuration. The **no names** command disables the use of the text names, but does not remove them from the configuration. The **show names** command lists the **name** command statements in the configuration.

Configuration Example

172.16.6.0

Internet **192.168.6.0** .1 **10.0.6.0** **10.1.6.0**

.2 .1 .1

Ethernet0
• Interface name = outside
• Security level = 0
• IP address = 192.168.6.2

Ethernet1
• Interface name = inside
• Security level = 100
• IP address = 10.0.6.1
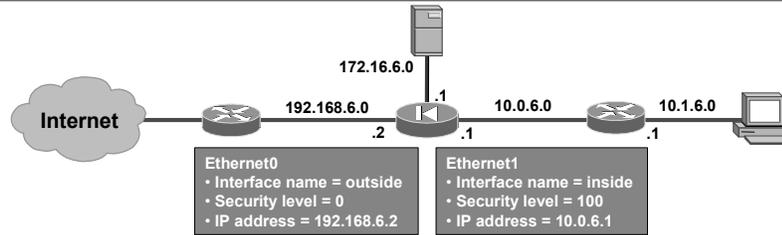
```
write terminal
interface ethernet0
  nameif outside
  security-level 0
  speed 100
  duplex full
  ip address 192.168.2.2 255.255.255.0
interface ethernet1
  nameif inside
  security-level 100
  speed 100
  duplex full
  ip address 10.0.1.1 255.255.255.0
```

SNPA v4.0—3-35

The figure shows a basic security appliance interface configuration. There are six configuration commands in the example, **interface**, **nameif**, **security-level**, **speed**, **duplex**, and **ip address**. Ethernet0 and Ethernet1 are set for their default name configuration: ethernet0, nameif outside, and security-level 0. All security appliance ports are set for 100-Mbps full-duplex communications. The last interface configuration subcommand is the **ip address** command. Each of the interfaces is assigned an IP address and subnet mask, for example, ip address outside 192.168.2.2 255.255.255.0. The configuration is continued on the next page.

Configuration Example (Cont.)

"bastionhost"
172.16.6.2

Ethernet2
• Interface name = dmz
• Security level = 50
• IP address = 172.16.6.1

"insidehost"
10.1.6.11

172.16.6.0

192.168.6.0   10.0.6.0   10.1.6.0

Internet

.1

.2   .1   .1
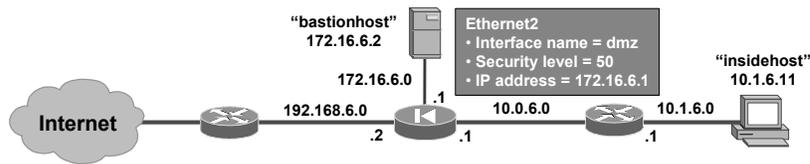
```
interface ethernet2
  nameif dmz
  security-level 50
  speed 100
  duplex full
  ip address 172.16.2.2 255.255.255.0
passwd 2KFQnbNIdI.2KYOU encrypted
hostname fw1
names
name 172.16.6.2 bastionhost
name 10.1.6.11 insidehost
```

In the previous configuration example, the interfaces are configured. In this figure, Ethernet2 is configured using the **nameif**, **security-level**, **speed**, **duplex**, and **ip address** subcommands. Hostname and names features are also configured. The hostname feature allows the administrator to define the CLI prompt, for example, fw1. The administrator can apply a name to any of the hosts, for example, 10.1.6.11 can be named insidehost. The configuration is continued on the next page.

Configuration Example (Cont.)
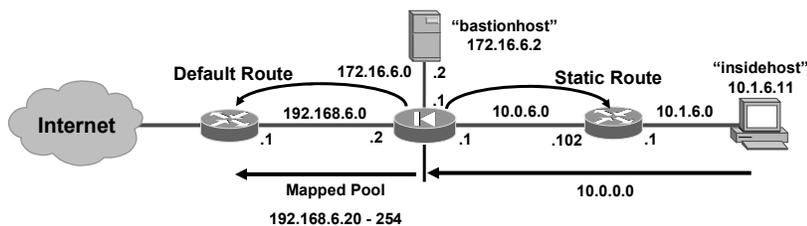
```
nat-control
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
global (outside) 1 192.168.6.20-192.168.6.254
route outside 0.0.0.0 0.0.0.0 192.168.6.1 1
route inside 10.1.6.0 255.255.255.0 10.0.6.102 1
```

SNPA v4.0—3-37

global and **nat** commands enable the NAT feature in the security appliance. In the example, outbound packets from any inside host, 0.0.0.0 0.0.0.0, are translated to one of the mapped pool IP addresses, 192.168.6.20–254. The last command is the **route** command. In the example, a default route to the router at IP address 192.168.6.1 is added. The hosts on the 10.1.6.0 network by default cannot be reached by the security appliance. To access these devices, a static route to the router at IP address 10.0.6.102 is defined. Any security appliance packets bound for the 10.1.6.0 network are forwarded to the router at IP address 10.0.6.102.

Examining Security Appliance Status

This topic contains the basic **show** commands needed to examine the status of Cisco security appliances.

show Commands

Cisco.com

show run interface

```
fw1# show run interface
!
interface Ethernet0
 speed 100
 duplex full
 nameif outside
 security-level 0
 ip address 192.168.2.2 255.255.255.0
!
interface Ethernet1
 speed 100
 duplex full
 nameif inside
 security-level 100
 ip address 10.0.2.1 255.255.255.0
```

show interface

```
fw1# show interface
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
        Detected: Speed 100 Mbps, Full-duplex
        Requested: Auto
        MAC address 000b.fcf8.c538, MTU 1500
        IP address 192.168.1.2, subnet mask 255.255.255.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 packets output, 0 bytes, 0 underruns
        input queue (curr/max blocks): hardware (0/0) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)
            Received 0 VLAN untagged packets, 0 bytes
            Transmitted 0 VLAN untagged packets, 0 bytes
            Dropped 0 VLAN untagged packets
```

SNPA v4.0—3-39

In general, **show run** plus a command displays a static screen, typically the way a parameter is configured. **show** plus a command displays a dynamically changing statistics screen. For example, **show run interface** displays how the interfaces are configured, a static screen. **show interface** displays a dynamic screen with numerous counters.

show memory Command

firewall#

```
show memory
```

```
fw1# show memory
Free memory:        49046552 bytes
Used memory:        18062312 bytes
-------------      ---------------
Total memory:       67108864 bytes
```

SNPA v4.0—3-40

The **show memory** command displays a summary of the maximum physical memory, current used memory, and current free memory available to the security appliance operating system. The example in the figure shows sample output from the **show memory** command.

show cpu usage Command
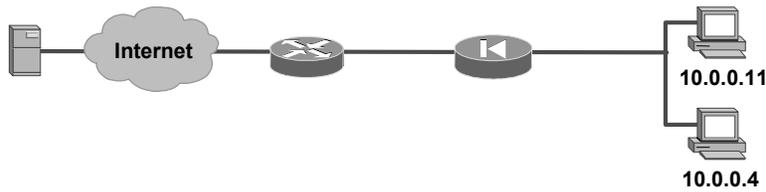
firewall#

```
show cpu usage
```

```
fw1# show cpu usage
CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%
```

SNPA v4.0—3-41

The **show cpu usage** command displays CPU use. In the following sample output for the **show cpu usage** command, 0% is the percentage of CPU used for five seconds, 0% is the average percentage of CPU use for one minute, and 0% is the average percentage utilization for five minutes:

```
CPU utilization for 5 seconds: 0%; 1 minute: 0%; 5 minutes: 0%
```

The percentage of usage shows as NA (not available) if the usage is not available for any of the time intervals. This can happen if the user asks for CPU usage before the five-second, one-minute, or five-minute time interval has elapsed.

show version Command

firewall#

```
show version
```

- **Displays the security appliance's software version, operating time since its last reboot, processor type, Flash memory type, interface boards, serial number (BIOS identification), and activation key value.**

```
Cisco PIX Security Appliance Software Version 7.0(1)

Compiled on Thu 31-Mar-05 14:37 by builders
System image file is "flash:/pix-701.bin"
Config file at boot was "startup-config"

pixfirewall up 12 mins 24 secs

Hardware:   PIX-515, 128 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 16MB...............
```

SNPA v4.0—3-42

Use the **show version** command to display the security appliance's software version, operating time since the last reboot, processor type, Flash memory type, interface boards, serial number (BIOS identification), and activation key value.

The serial number listed with the **show version** command in Cisco PIX Security Appliance Software v5.3 and higher is for the Flash memory basic input/output system (BIOS). This number is different from the serial number on the chassis. To obtain a software upgrade, you need the serial number that appears in the **show version** command, not the chassis number.

For Cisco PIX and ASA Security Appliance Software v7.0 and higher, the **show version** output appears as follows:

```
pix1# show version

Cisco PIX Security Appliance Software Version 7.0(1)

Compiled on Thu 31-Mar-05 14:37 by builders
System image file is "flash:/pix-701.bin"
Config file at boot was "startup-config"

pix1 up 12 mins 24 secs

Hardware:   PIX-515, 128 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 16MB
BIOS Flash AT29C257 @ 0xfffd8000, 32KB

 0: Ext: Ethernet0              : media index  0: irq 10
 1: Ext: Ethernet1              : media index  1: irq 7
 2: Ext: Ethernet2              : media index  2: irq 11
 3: Ext: Ethernet3              : media index  3: irq 11
 4: Ext: Ethernet4              : media index  4: irq 11
```

```
       5: Ext: Ethernet5          : media index  5: irq 11

       Licensed features for this platform:
       Maximum Physical Interfaces : 6
       Maximum VLANs               : 25
       Inside Hosts                : Unlimited
       Failover                    : Active/Active
       VPN-DES                     : Enabled
       VPN-3DES-AES                : Enabled
       Cut-through Proxy           : Enabled
       Guards                      : Enabled
       URL Filtering               : Enabled
       Security Contexts           : 5
       GTP/GPRS                    : Disabled
       VPN Peers                   : Unlimited


       This platform has an Unrestricted (UR) license.


       Serial Number: 480360257
       Running Activation Key: 0x4431d243 0x54258b0f 0x90913408
       0xb6bcd404 0x8f37eaac
       Configuration has not been modified since last system restart.
```

In the above example, notice the following important bolded parameters:

```
Hardware:          PIX-515, 128 MB RAM
Flash:             16MB
Licensed Features:
Failover:          Active/Active
VPN-DES:           Enabled
VPN-3DES-AES:      Enabled
Security Contexts  5
This PIX 515 Security Appliance has an Unrestricted (UR) license.
Serial Number: 480360257
```

show ip address Command

172.16.6.0

Internet

192.168.6.0   10.0.6.0   10.1.6.0

.1

.2   .1   .1
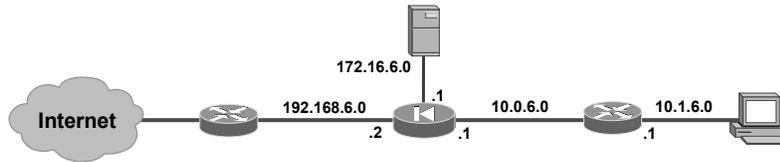
```
fw1# show ip address
System IP Addresses:
Interface       Name            IP address      Subnet mask
Ethernet0       outside         192.168.1.2     255.255.255.0
CONFIG
Ethernet1        inside          10.0.1.1        255.255.255.0
CONFIG
Ethernet2       dmz             172.16.1.1      255.255.255.0
CONFIG
Current IP Addresses:
Interface       Name            IP address      Subnet mask
Ethernet0        outside         192.168.1.2     255.255.255.0
CONFIG
Ethernet1        inside          10.0.1.1        255.255.255.0
CONFIG
Ethernet2       dmz             172.16.1.1      255.255.255.0
CONFIG
```

SNPA v4.0—3-43

The **show ip address** command enables you to view which IP addresses are assigned to the network interfaces. The current IP addresses are the same as the system IP addresses on the failover active security appliance. When the active security appliance fails, the current IP addresses become that of the standby security appliance.

show interface Command

```
fw1# show interface
interface ethernet0 "outside" is up, line protocol is up
  Hardware is i82559 ethernet, address is 0050.54ff.653a
  IP address 192.168.0.2, subnet mask 255.255.255.0
  MTU 1500 bytes, BW 100000 Kbit full duplex
        4 packets input, 282 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        20 packets output, 1242 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0
        output queue (curr/max blocks): hardware (0/1) software (0/1)
```

SNPA v4.0—3-44

The **show interface** command enables you to view network interface information. This is one of the first commands you should use when trying to establish connectivity.

The following are explanations of the information that is displayed after you enter the **show interface** command:

■ Ethernet: Indicates that you have used the **interface** command to configure the interface. The statement indicates whether the interface is inside or outside and whether the interface is available (up) or not available (down).

■ Line protocol up: A working cable is plugged into the network interface.

■ Line protocol down: Either the cable plugged into the network interface is incorrect or it is not plugged into the interface connector.

■ Network interface type: Identifies the network interface.

■ MAC address: Intel cards begin with "i" and 3Com cards begin with "3c".

■ MTU (maximum transmission unit): The size in bytes that data can best be sent over the network.

■ Line speed: 10BASE-T is listed as 10000 Kbit. 100BASE-TX is listed as 100000 Kbit.

■ Line duplex status: Indicates whether the security appliance is running either full duplex (simultaneous packet transmission) or half duplex (alternating packet transmission).

■ Packets input: Indicates that packets are being received in the security appliance.

■ Packets output: Indicates that packets are being sent from the security appliance.

The following are explanations of **show interface** command output that can indicate interface problems:

- No buffer: Indicates the security appliance is out of memory or slowed down due to heavy traffic and cannot keep up with the received data.

- Runts: Packets with less information than expected.

- Giants: Packets with more information than expected.

- CRC (cyclic redundancy check): Packets that contain corrupted data (checksum error).

- Frame errors: Indicates framing errors.

- Ignored and aborted errors: This information is provided for future use, but is not currently checked; the security appliance does not ignore or abort frames.

- Underruns: Occurs when the security appliance is overwhelmed and cannot get data to the network interface card fast enough.

- Overruns: Occurs when the network interface card is overwhelmed and cannot buffer received information before more needs to be sent.

- Unicast rpf drops: Occurs when packets sent to a single network destination using reverse path forwarding are dropped.

- Output errors (maximum collisions): The number of frames not transmitted because the configured maximum number of collisions was exceeded. This counter should only increment during heavy network traffic.

- Collisions (single and multiple collisions): The number of messages retransmitted because of an Ethernet collision. This usually occurs on an overextended LAN when the Ethernet or transceiver cable is too long, there are more than two repeaters between stations, or there are too many cascaded multiport transceivers. A packet that collides is counted only once by the output packets.

- Interface resets: The number of times an interface has been reset. If an interface is unable to transmit for three seconds, the security appliance resets the interface to restart transmission. During this interval, the connection state is maintained. An interface reset can also happen when an interface is looped back or shut down.

- Babbles: The transmitter has been on the interface longer than the time taken to transmit the largest frame. This counter is unused.

- Late collisions: The number of frames that were not transmitted because a collision occurred outside the normal collision window. A late collision is a collision that is detected late in the transmission of the packet. Normally, these should never happen. When two Ethernet hosts try to talk at once, they should collide early in the packet and both back off, or the second host should see that the first one is talking and wait.

If you get a late collision, a device is jumping in and trying to send on the Ethernet while the security appliance is partly finished sending the packet. The security appliance does not resend the packet, because it may have freed the buffers that held the first part of the packet. This is not a real problem because networking protocols are designed to cope with collisions by resending packets. However, late collisions indicate a problem exists in your network. Common problems are large repeated networks and Ethernet networks running beyond the specification.

- Deferred: The number of frames that were deferred before transmission because of activity on the link.

- Lost carrier: The number of times the carrier signal was lost during transmission.

- No carrier: This counter is unused.

- Input queue: Input (receive) hardware and software queue.

  — Hardware (current and maximum blocks): The number of blocks currently present on the input hardware queue and the maximum number of blocks previously present on that queue.

  — Software (current and maximum blocks): The number of blocks currently present on the input software queue and the maximum number of blocks previously present on that queue.

- Output queue: Output (transmit) hardware and software queue.

  — Hardware (current and maximum blocks): The number of blocks currently present on the output hardware queue and the maximum number of blocks previously present on that queue.

  — Software (current and maximum blocks): The number of blocks currently present on the output software queue and the maximum number of blocks previously present on that queue.

Note   The following counters are valid only for Ethernet interfaces: output errors, collisions, interface resets, babbles, late collisions, deferred, lost carrier, and no carrier.

Note   Starting with PIX Security Appliance Software v6.0(1), Fiber Distributed Data Interface (FDDI), Private Link 2 (PL2), and Token Ring interfaces are not supported.

---

show nameif Command

Ethernet2
• Interface name = dmz
• Security level = 50

Internet

e2

e0   e1

Ethernet0
• Interface name = outside
• Security level = 0

Ethernet1
• Interface name = inside
• Security level = 100
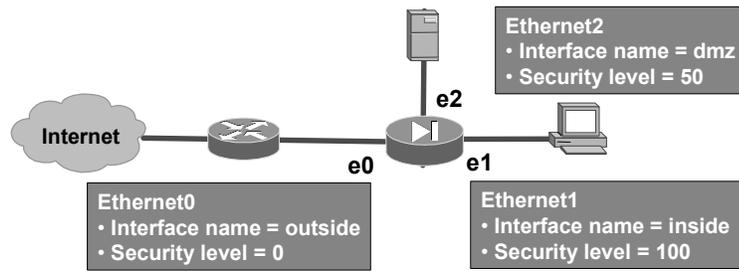
```
fw1# show nameif
Interface         Name              Security
Ethernet0         outside              0
Ethernet1         inside             100
Ethernet2         dmz                 50
```

SNPA v4.0—3-45

Use the **show nameif** command to view the named interfaces. In the figure, the first two interfaces have the default names **inside** and **outside**. The **inside** interface has a default security level of 100; the **outside** interface has a default security level of 0. Ethernet2 is assigned a name of **dmz** with a security level of 50.

show run nat Command

Internet

10.0.0.11

X.X.X.X   10.0.0.X

NAT

10.0.0.4
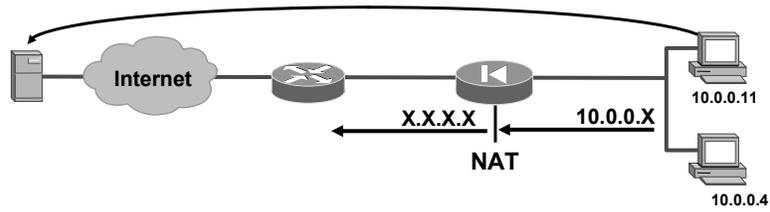
firewall#

```
show run nat
```

- **Displays a single host or range of hosts to be translated**

```
fw1# show run nat
nat (inside) 1 10.0.0.0 255.255.255.0 0 0
```

SNPA v4.0—3-46

Use the **show run nat** command to display a single host or range of hosts to be translated. In the figure, all hosts on the 10.0.0.0 network will be translated when traversing the security appliance. The NAT ID is 1.

show run global Command

Cisco.com
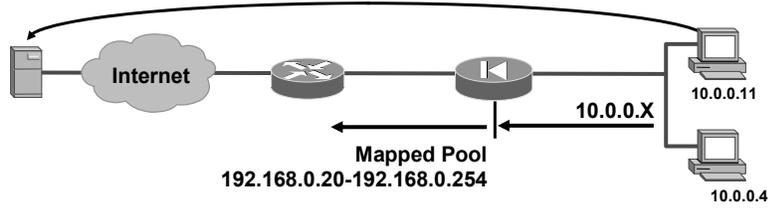
```
firewall#
```

```
show run global
```

- **Displays the pool of mapped addresses**

```
fw1# show run global
global (outside) 1 192.168.0.20-192.168.0.254 netmask 255.255.255.0
```

SNPA v4.0—3-47

Show run global displays the mapped pool(s) of addresses configured in the security appliance. The figure shows one pool currently configured. The pool is configured on the outside interface. The pool has an IP address range of 192.168.0.20 to 192.168.0.254. The NAT ID is 1.

show xlate Command

Cisco.com

Internet

192.168.0.20   10.0.0.11

10.0.0.11

10.0.0.4

Xlate Table

Outside mapped pool	Inside local
192.168.0.20	10.0.0.11
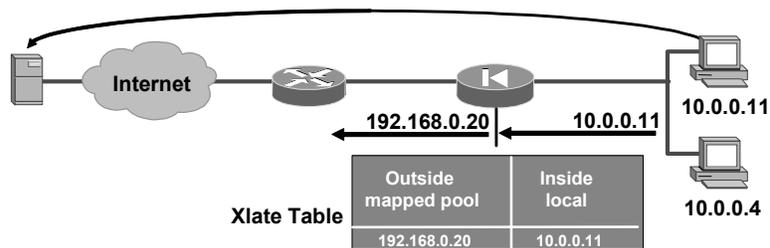
firewall#

```
show xlate
```

• **Displays the contents of the translation slots**

```
fw1# show xlate
1 in use, 1 most used
Global 192.168.0.20 Local 10.0.0.11
```

SNPA v4.0—3-48

The command **show xlate** displays the contents of the translation slot. In the figure, the number of currently used translations is 1 with a maximum count of 1. The current translation is a local IP address of 10.0.0.11 to a mapped IP address of 192.168.0.20.

ping Command

Internet

10.0.0.11

10.0.0.4
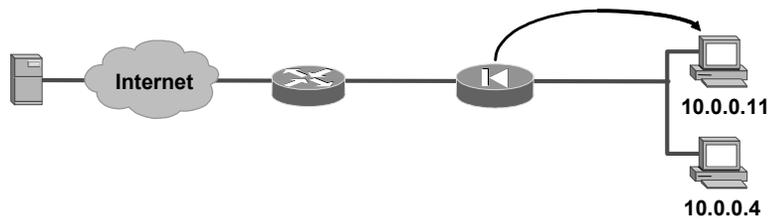
firewall#

```
ping host
```

- **Determines whether other IP addresses are visible from the security appliance**

```
fw1# ping 10.0.1.11
Sending 5, 100-byte ICMP Echos to 10.0.1.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/12/20 ms
```

SNPA v4.0—3-49

The **ping** command determines if the security appliance has connectivity and if a host is available (visible to the security appliance) on the network. The command output shows if the ping was received. If the ping was received, then the host exists on the network. If the ping was not received, the command output displays "NO response received." (In that case, you would use the **show interface** command to ensure that the security appliance is connected to the network and is passing traffic.) By default, the **ping** command makes three attempts to reach an IP address.

If you want internal hosts to be able to ping external hosts, you must create an ACL for echo reply. If you are pinging through the security appliance between hosts or routers and the pings are not successful, use the **debug icmp trace** command to monitor the success of the ping.

After your security appliance is configured and operational, you will not be able to ping the inside interface of the security appliance from the outside network or from the outside interfaces of the security appliance. If you can ping the inside networks from the inside interface and if you can ping the outside networks from the outside interface, the security appliance is functioning normally and your routes are correct.

The syntax for the **ping** command is as follows:

```
ping [if_name] host [data pattern] [repeat count] [size bytes]
[timeout seconds] [validate]
```

if_name	The network interface name. The address of the specified interface is used as the source address of the ping.
host	The name or IP address of the host being pinged.
data *pattern*	(Optional) Specifies the 16-bit data pattern in hexadecimal.
repeat *count*	(Optional) Specifies the number of times to repeat the ping request.
size *bytes*	(Optional) Specifies the datagram size in bytes.
timeout *seconds*	(Optional) Specifies the number of seconds to wait before timing out the ping request.
validate	(Optional) Specifies to validate reply data.

Time Setting and NTP Support

This topic explains how to set the clock on the security appliance and synchronize the times of devices operating over an IP data network.

clock Command

Cisco.com

Internet

Wed 23-Jul-03
21:00

10.0.0.11

10.0.0.4
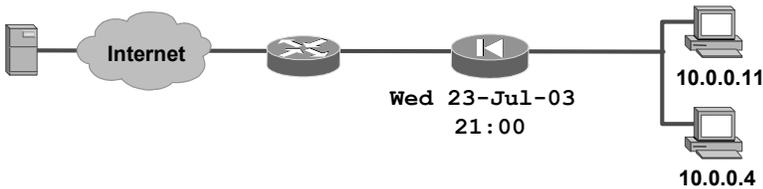
```
firewall#
clock set hh:mm:ss {day month | month day} year
```

• **Sets the security appliance clock**

```
fw1# clock set 21:0:0 jul 23 2003
```

SNPA v4.0—3-52

The **clock set** command sets the security appliance clock. It enables you to specify the time, month, day, and year. The clock setting is retained in memory when the power is off by a battery on the security appliance's motherboard. The security appliance generates syslog messages for system events and can log these messages to a syslog server. If you want the messages to contain a time-stamp value, you must enter the **logging timestamp** command. The **logging timestamp** command requires that the **clock set** command be used to ensure that the correct time appears on the Syslog messages. Syslog and its corresponding commands are explained in another lesson.

It is also important to ensure that the clock is correctly set if you use public key infrastructure (PKI), which uses digital certificates for authentication of virtual private network (VPN) peers. The Cisco PKI protocol uses the clock to make sure that a certificate revocation list (CRL) is not expired. Otherwise, the certificate authority (CA) may reject or allow certificates based on an incorrect time stamp. The lifetimes of certificates and CRLs are checked in Coordinated Universal Time (UTC). If you are using certificates with IPSec for VPNs, set the security appliance clock to UTC time zone to ensure that CRL checking works correctly.

You can view the time with the **show clock** command, which displays the time, time zone, day, and full date. You can remove the **clock set** command with the **clear configure clock** command.

The syntax for the **clock set** command is as follows:

```
clock set hh:mm:ss {month day | day month} year
```

hh:mm:ss	The hour: minutes: seconds expressed in 24-hour time (for example, 20:54:00 for 8:54 p.m.). Zeros can be entered as a single digit; for example, 21:0:0.
day	The day of the month to start, from 1 to 31.
month	The month expressed as the first three characters of the month (for example, apr for April).
year	The year expressed as four digits (for example, 2000).

Setting Daylight Saving Time and Time Zones

firewall(config)#

```
clock summer-time zone recurring [week weekday
  month hh:mm week weekday month hh:mm] [offset]
```

- **Displays summertime hours during the specified summertime date range**

firewall(config)#

```
clock timezone zone hours [minutes]
```

- **Sets the clock display to the time zone specified**

```
fw1(config)# clock summer-time PDT recurring 1 Sunday April 2:00 last Sunday
  October 2:00
```

- **Specifies that summertime starts on the first Sunday in April at 2 a.m. and ends on the last Sunday in October at 2 a.m.**

SNPA v4.0—3-53

Although the security appliance clock does not adjust itself for daylight saving time changes, you can configure it to display daylight saving time by using the **clock summer-time** command. The **summer-time** keyword causes the security appliance to automatically switch to summertime (for display purposes only). The **recurring** keyword indicates that summertime should start and end on the days that are specified by the values that follow it. If no values are specified, the summertime rules default to U.S. rules.

You can also specify the exact date and times with the **date** version of the **clock summer-time** command. In the following example, daylight saving time (summertime) is configured to start on April 7, 2002, at 2 a.m. and end on October 27, 2002, at 2 a.m.

```
fw1 (config)# clock summer-time PDT date 7 April 2002 2:00 27
October 2002 2:00
```

Use the **clock timezone** command to set the time zone. The **clock timezone** command sets the time zone for display purposes only. Internally, the time is kept in UTC. The **no** form of the command is used to set the time zone to UTC. The **clear clock** command removes summertime settings and sets the time zone to UTC.

The syntax for the **clock** commands is as follows:

```
clock summer-time zone recurring [week weekday month hh:mm
week weekday month hh:mm] [offset]
clock summer-time zone date {day month | month day} year hh:mm
{day month | month day} year hh:mm [offset]
clock timezone zone hours [minutes]
show clock [detail]
```

summer-time	The **clock summer-time** command displays summertime hours during the specified summertime date range. This command affects the clock display time only.
zone	The name of the time zone.
recurring	Specifies the start and end dates for local summer "daylight saving" time. The first date entered is the start date and the second date entered is the end date. (The start date is relative to UTC and the end date is relative to the specified summer time zone.) If no dates are specified, U.S. Daylight Saving Time is used. If the start-date month is after the end-date month, the summer time zone is accepted and assumed to be in the Southern Hemisphere.
week	Specifies the week of the month. Enter 1, 2, 3, or 4 to specify the first, second, third, or fourth week of the month. Use first or last to specify a partial week at the beginning or end of a month. For example, week 5 of any month is specified by using last.
weekday	Specifies the day of the week. Enter **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, or **Sunday**.
month	Specifies the month. Enter the first three characters of the month (for example, **apr** for April).
hh:mm	The hour and minutes expressed in 24-hour time (for example, 20:54 for 8:54 p.m.). Zeros can be entered as a single digit (for example, 21:0).
offset	The number of minutes to add during summertime. The default is 60 minutes.
date	Used as an alternative to the recurring form of the **clock summer-time** command. It specifies that summertime should start on the first date entered and end on the second date entered. If the start-date month is after the end-date month, the summer time zone is accepted and assumed to be in the Southern Hemisphere.
day	The day of the month to start. Enter a number from 1 to 31.
year	The year expressed as four digits (for example, **2000**). The year range supported for the **clock** command is 1993 to 2035.
timezone	The **clock timezone** command sets the clock display to the time zone specified. It does not change internal security appliance time, which remains UTC.
hours	The hours of offset from UTC.
minutes	The minutes of offset from UTC.
detail	Displays the clock source and current summertime settings.

ntp Command
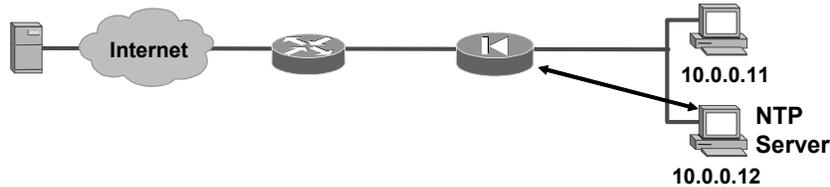
firewall(config)#

```
ntp server ip_address [key number] source if_name
  [prefer]
```

- **Synchronizes the security appliance with an NTP server**

```
fw1(config)# ntp authentication-key 1234 md5 cisco123
fw1(config)# ntp trusted-key 1234
fw1(config)# ntp server 10.0.0.12 key 1234 source inside prefer
fw1(config)# ntp authenticate
```

SNPA v4.0—3-54

The **ntp server** command synchronizes the security appliance with the NTP server that you specify. You can configure the security appliance to require authentication before synchronizing with the NTP server. To enable and support authentication, several forms of the **ntp** command work in conjunction with the **ntp server** command. The following are the **ntp** command forms and their uses:

- **ntp server**: Specifies an NTP server. The security appliance listens for NTP packets (port 123) only on interfaces that have an NTP server configured. NTP packets that are not responses from a request by the security appliance are dropped.

- **ntp authenticate**: Enables NTP authentication.

- **ntp authentication-key**: Defines the authentication keys for the **ntp** commands. If authentication is used, the security appliance and NTP server must be configured with the same key.

- **ntp trusted-key**: Defines one or more key numbers that the NTP server needs to include in its NTP packets in order for the security appliance to accept synchronization with the NTP server. Use this command if NTP authentication is enabled.

You can use the **show run ntp** command to display the current NTP configuration and the **show ntp status** command to display the NTP clock information. The **clear configure ntp** command removes the NTP configuration, including disabling authentication and removing all authentication keys and NTP server designations.

The syntax for the **ntp** commands is as follows:

```
ntp authenticate
ntp authentication-key number md5 value
ntp server ip_address [key number] source if_name [prefer]
ntp trusted-key number
```

authenticate	Enables NTP authentication. If enabled, the security appliance requires authentication before synchronizing with an NTP server.
authentication-key	Defines the authentication keys for use with other NTP commands.
number	The authentication key number (1 to 4294967295).
md5	The authentication algorithm.
value	The key value, an arbitrary string of up to 32 characters. The key value is displayed as "************" when the configuration is viewed by using the **show run** or **show tech-support** command.
server	The NTP server.
ip_address	The IP address of the NTP server with which to synchronize.
key	Specifies the authentication key.
source	Specifies the network time source.
if_name	Specifies the interface to use to send packets to the NTP server.
prefer	Designates the NTP server specified as the preferred server with which to synchronize time.
trusted-key	Specifies the trusted key against which to authenticate.

Syslog Configuration

This topic explains how to configure Cisco security appliances to send syslog messages to a syslog server.

The security appliance generates syslog messages for system events, such as alerts and resource depletion. Syslog messages can be used to create log files or can be displayed on the console of a designated syslog host. The security appliance can send syslog messages to any syslog server. In the event that all syslog servers or hosts are offline, the security appliance syslog server stores up to 512 messages in its memory. Subsequent messages that arrive overwrite the buffer starting from the first line.

Logging Options

Console – Output to console

Buffered – Output to internal buffer

Logging Options → Monitor – Output to Telnet

Host – Output to syslog server

SNMP – Output to SNMP server

SNPA v4.0—3-57

These are some of the logging options available on Cisco security appliances.

- Console: Specifies that given log messages appear on the security appliance console as each message occurs

- Buffered: Sends the specified log messages to an internal buffer that can be viewed with the **show logging** command

- Monitor: Specifies that the log messages appear on Telnet sessions to the security appliance console

- Host: Specifies which log server will receive the messages that are sent from the security appliance

- Simple Network Management Protocol (SNMP): Enables sending log messages as SNMP trap notifications
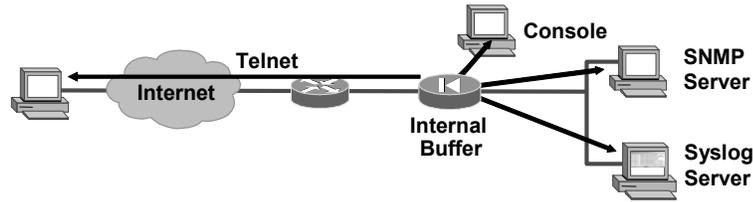
SNPA v4.0—3-58

The level that you specify indicates that you want *that* level and all higher levels. For example, if the log level is 3, the syslog displays 0, 1, 2, and 3 messages**.** Possible number and string level values are as follows:

- **0: Emergencies**—System unusable messages

- **1**: **Alerts**—Take immediate action

- **2: Critical**—Critical condition

- **3: Errors**—Error message

- **4: Warnings**—Warning message

- **5: Notifications**—Normal but significant condition

- **6: Informational**—Information message

- **7: Debugging**—Debug messages and log FTP commands and World Wide Web URLs

Configure Message Output to a Syslog Server

Cisco.com

fw1

Internet

Syslog Messages

Syslog Server
10.0.1.11
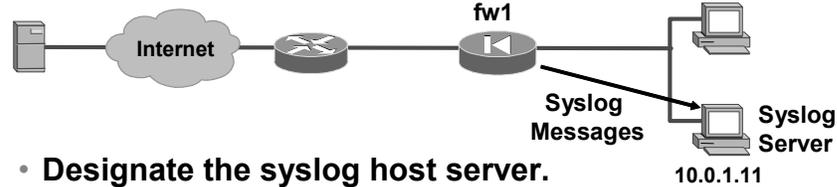
- **Designate the syslog host server.**
- **Set the logging level.**
- **Enable logging time stamp on syslog messages.**
- **Specify the logging device identifier.**
- **Enable logging.**

```
fw1(config)# logging host inside 10.0.1.11
fw1(config)# logging trap warnings
fw1(config)# logging timestamp
fw1(config)# logging device-id pix6
fw1(config)# logging on
```

SNPA v4.0—3-59

In the figure, the security appliance is configured to send the logging messages to syslog server 10.0.0.12. The messages that are sent will consist of warning messages and messages of higher severity. Each message is time-stamped and assigned a device identifier of pix6. Lastly, logging is turned on.

Syslog Output Example

In the example syslog output, the administrator can view the following information:

- Priority: The security appliance message logging level, for example, debug.

- Hostname: The IP address of the security appliance, for example, 10.0.6.1.

- Message: The message sent from the security appliance. The message includes the following information:

    — Logging date and time stamp, for example, Aug 05 2003 14:51:04

    — Logging device identifier, for example, pix6

    — Message identifier, for example, 71005

    — Message text, for example, a UDP request discarded from 10.0.6.10/137 to inside: 10.0.6.255/netbios-ns

Customize Syslog Output

firewall(config)#

```
no logging message syslog_id
```

- **Disallows unwanted syslog messages**

```
fw1(config)# no logging message 710005
```

firewall(config)#

```
logging message syslog_id level level
```

- **Enables you to change the level of specific syslog messages**

```
fw1(config)# logging trap warnings
fw1(config)# logging message 302013 level 4
fw1(config)# logging message 302014 level 4
```

SNPA v4.0—3-61

You can use the **logging message** command to customize the syslog output from the security appliance. If the syslog is flooded with a number of unwanted event messages, such as netbios messages, you can block the output of these event messages by using the **no logging message syslog_id** command. In the top example in the figure, the syslog is flooded with netbios message 710005. You can block the security appliance from sending the message by configuring the **no logging message** *syslog_id* command where 710005 is *syslog_id*.

If you set the logging trap level to debug, the syslog is flooded with event messages. If the level is raised to warning, the good news is the number of syslog event messages decreases significantly. The bad news is that some of the level 5, 6, and 7 syslog messages you may want to view are no longer output by the security appliance. You can view the suppressed messages by changing the logging level on the message. In the lower example in the figure, the security appliance is configured to forward only warning messages and above, levels 1 through 4. You are unable to view selected syslog messages from levels 5 through 7, such as %PIX-**6-302013** built outbound TCP connection and %PIX-**6-302014** teardown TCP connection. By changing the 302013 and 302014 message levels to level 4, the security appliance will start to output syslog messages 302013 and 302014 to the syslog server.

show logging Command
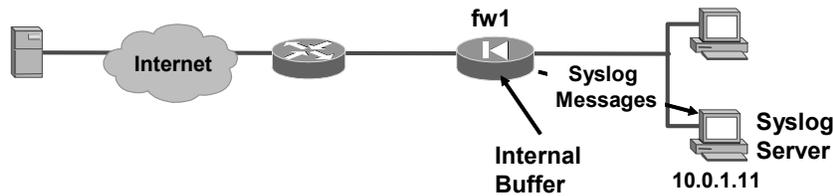
```
fw1(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: enabled
    Standby logging: disabled
    Ambiguous interface parameters: 97
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: level warnings, 0 messages logged
    Trap logging: level warnings, facility 20, 0 messages logged
        Logging to inside 10.0.1.11
    History logging: disabled
    Device ID: fw1
    Mail logging: disabled
    PDM logging: disabled
```

SNPA v4.0—3-62

Use the **show logging** command to see the logging configuration and any internally buffered messages. Use the **clear logging buffer** command to clear the buffer to make viewing the most current messages easier. In the figure, logging is enabled. The security appliance will send warning messages and messages of higher severity to a syslog server and the security appliance internal buffer. On syslog messages, the fw1 device identifier and a time stamp will be appended.

Summary

This topic summarizes what you learned in this lesson.

Summary

- **Cisco security appliances have four administrative access modes: unprivileged, privileged, configuration, and monitor.**
- **Interfaces with a higher security level can access interfaces with a lower security level, but interfaces with a lower security level cannot access interfaces with a higher security level unless given permission.**
- **The security appliance** show **commands help you manage the security appliance.**

SNPA v4.0—3-63

Summary (Cont.)

- **The basic commands that are necessary to configure Cisco security appliances are the following: *interface*, *nameif*, *nat*, *global*, and *route*.**
- **The *nat* and *global* commands work together to translate IP addresses.**
- **The security appliance can send syslog messages to a syslog server.**
- **The security appliance can function as a DHCP client.**

SNPA v4.0—3-64

Lesson 4

Translations and Connections

Overview

This lesson discusses security appliance translations and connections. First, it shows how Cisco security appliances process TCP and User Datagram Protocol (UDP) traffic. Then it shows how to configure dynamic and static address translations in a security appliance.

Objectives

Upon completion of this lesson, you will be able to perform address translation on a security appliance. This includes being able to meet these objectives:

- Describe how the TCP and UDP protocols function within the security appliance

- Describe how static and dynamic translations function

- Configure dynamic address translation

- Configure static address translation

- Describe TCP intercept features and configure connection limits

- Describe how to configure address translation across multiple interfaces

Transport Protocols

This topic aids in understanding TCP and UDP. You need to understand these transport protocols to understand how the security appliance operates.

Sessions in an IP World

In an IP world, a network session is a transaction between two end systems. It is carried out primarily over two transport layer protocols:

- **TCP**
- **UDP**

SNPA v4.0—4-3

A network session is carried out over two transport layer protocols:

- TCP: easy to inspect

- UDP: state of a session is difficult to maintain as it has no clear beginning, flow state, or end

---

Note   In the context of this training, the term *outbound* means connections from a more trusted side of the security appliance to a less trusted side of the security appliance. The term *inbound* means connections from a less trusted side of the security appliance to a more trusted side of the security appliance.

TCP

- **TCP is a connection-oriented, reliable-delivery, robust, and high-performance transport layer protocol.**
- **TCP features:**
  - **Sequencing and acknowledgment of data**
  - **A defined state machine (open connection, data flow, retransmit, close connection)**
  - **Congestion detection and avoidance mechanisms**

SNPA v4.0—4-4

TCP is a connection-oriented protocol. When a session from a more secure host inside the security appliance is started, the security appliance creates an entry in the session state filter. The security appliance is able to extract network sessions from the network flow and actively verify their validity in real time. This stateful filter maintains the state of each network connection and checks subsequent protocol units against its expectations. When a TCP session is initiated through a security appliance, the security appliance records the network flow and looks for an acknowledgment from the device that the host is trying to initiate communications with. The security appliance then allows traffic to flow between the hosts that are involved in the connection based on the three-way handshake.

TCP Initialization: Inside to Outside

Private Network

Source Address	10.0.0.11
Destination Address	172.30.0.50
Source Port	1026
Destination Port	23
Initial Sequence #	49091
ACK	
Flag	Syn

The security appliance checks for a translation slot. If one is not found, it creates one after verifying NAT, global, access control, and authentication or authorization, if any. If OK, a connection is created.

Security Appliance

Start the *embryonic* connection counter.

Public Network

	192.168.0.20
	172.30.0.50
	1026
	23
	49769
	Syn

10.0.0.11   # 1   No Data   # 4

172.30.0.50   # 2   # 3

| 172.30.0.50 |
| 10.0.0.11 |
| 23 |
| 1026 |
| 92513 |
| 49092 |
| Syn-Ack |

The security appliance utilizes the stateful packet inspection algorithm:
- Source IP, source port, destination IP, destination port check
- Sequence number check
- Translation check

| 172.30.0.50 |
| 192.168.0.20 |
| 23 |
| 1026 |
| 92513 |
| 49770 |
| Syn-Ack |

IP Header

TCP Header

SNPA v4.0—4-5

When a TCP session is established over the security appliance, the following happens:

Step 1 The first IP packet from an inside host causes the generation of a translation slot. The embedded TCP information is then used to create a connection slot in the security appliance.

Step 2 The connection slot is marked as *embryonic* (not established yet).

Step 3 The security appliance randomizes the initial sequence number of the connection, stores the delta value, and forwards the packet onto the outgoing interface.

The security appliance now expects a synchronization-acknowledgment (SYN-ACK) packet from the destination host. Then the security appliance matches the received packet against the connection slot, computes the sequencing information, and forwards the return packet to the inside host.

TCP Initialization: Inside to Outside (Cont.)

Private Network

Source Address	10.0.0.11
Destination Address	172.30.0.50
Source Port	1026
Destination Port	23
Initial Sequence #	49092
ACK	92514
Flag	Ack

Public Network

192.168.0.20
172.30.0.50
1026
23
49770
92514
Ack

The security appliance Reset the embryonic counter for this client.. It then increases the connection counter for this host.

Security Appliance

The security appliance Strictly enforces the stateful packet inspection algorithm.

10.0.0.11

 # 5

Data Flows

 # 6

172.30.0.50

IP Header

TCP Header

SNPA v4.0—4-6

Step 1   The inside host completes the connection setup, the three-way handshake, with an ACK.

Step 2   The connection slot on the security appliance is marked as connected, or active-established, and data is transmitted. The embryonic counter is then reset for this connection.

UDP

- **Connectionless protocol**
- **Efficient protocol for some services**
- **Resourceful, but difficult to secure**

SNPA v4.0—4-7

UDP is connectionless. The security appliance must take other measures to ensure its security. Applications using UDP are difficult to secure properly because there is no handshaking or sequencing. It is difficult to determine the current state of a UDP transaction. It is also difficult to maintain the state of a session because it has no clear beginning, flow state, or end. However, the security appliance creates a UDP connection slot when a UDP packet is sent from a more secure to a less secure interface. All subsequent returned UDP packets that match the connection slot are forwarded to the inside network.

UDP (Cont.)

Private Network

Source Address	10.0.0.11
Destination Address	172.30.0.50
Source Port	1028
Destination Port	45000

The security appliance checks for a translation slot. If one is not found, it creates one after verifying NAT, global, access control, and authentication or authorization, if any. If OK, a connection is created.

Security Appliance

All UDP responses arrive from outside and within UDP user-configurable timeout (default is 2 minutes).

The security appliance follows the stateful packet inspection algorithm:
- Source IP, source port, destination IP, destination Port check
- Translation check

Public Network

192.168.0.20
172.30.0.50
1028
45000

10.0.0.11   # 1   # 2   172.30.0.50

4   # 3

172.30.0.50
10.0.0.11
45000
1028

172.30.0.50
192.168.0.20
45000
1028

IP Header
UDP Header

SNPA v4.0—4-8

When the UDP connection slot is idle for more than the configured idle time, it is deleted from the connection table. The following are some UDP characteristics:

- UDP is an unreliable, but efficient transport protocol.

- Spoofing UDP packets is very easy because there is no handshaking or sequencing. As there is no state machine, the initiator of the transaction or the current state usually cannot be determined.

- UDP has no delivery guarantees.

- There is no connection setup and termination.

- UDP has no congestion management or avoidance.

Services that use UDP can be generally divided into two categories:

- Request-reply, or ping-pong services, such as Domain Name System (DNS).

- Flow services, such as video, Voice over IP (VoIP), and Network File System (NFS).

Network Address Translation

This topic describes the translation process in Cisco security appliances. There are two types of inside translations: dynamic and static.

Addressing Scenarios

NAT

192.168.6.9   10.0.0.11

Internet

10.0.0.11

10.0.0.4

- **NAT was created to overcome several addressing problems that occurred with the expansion of the Internet:**
  - **To mitigate global address depletion**
  - **To use RFC 1918 addresses internally**
  - **To conserve internal address plan**
- **NAT also increases security by hiding the internal topology.**

SNPA v4.0—4-10
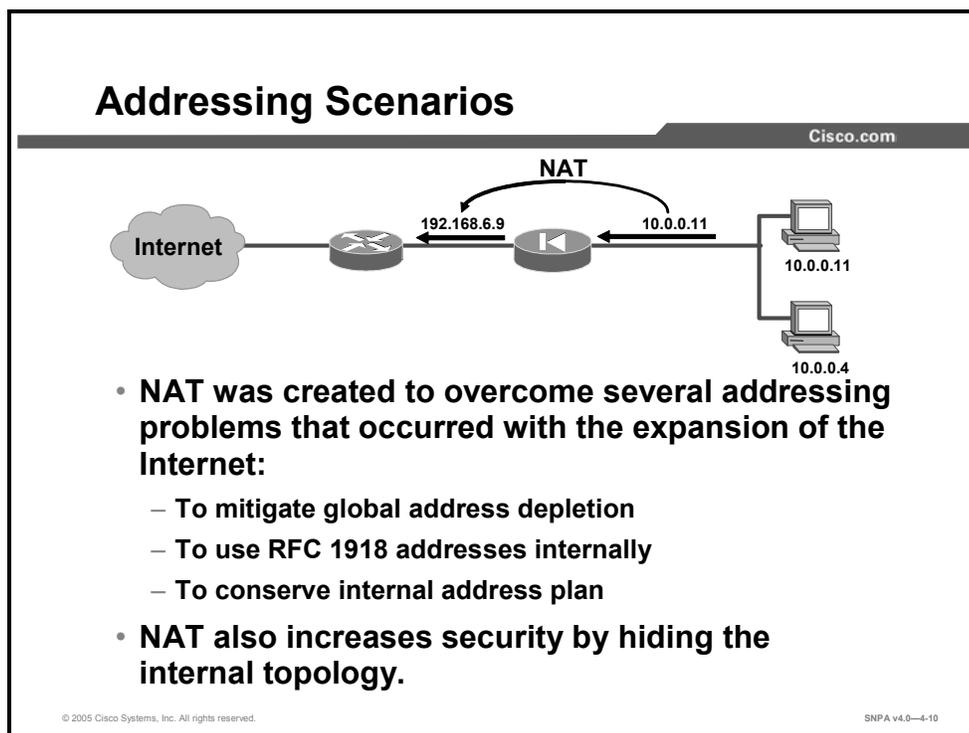
Invented in May 1994 by Paul Francis and Kjeld Borch Egevang, Network Address Translation (NAT) became a popular technique for saving official network addresses and hiding network topology from the Internet. Francis and Egevang have written several Request For Comments (RFCs) about NAT, the most important of which is RFC 1631, The IP Network Address Translator (NAT).

In the modern world, NAT is critical to the mitigation of global Internet address depletion. Very often, private networks are assigned numbers from network blocks defined in RFC 1918. Because these addresses are intended for local use only, NAT is required to connect to the Internet. NAT is sometimes used to preserve the inside addresses of an enterprise, for example, when changing the ISP.

In the figure, the private network is using private IP addressing, 10.0.0.0/24. Before a packet can be sent to the Internet, it must be translated into a public, routable address. In this example, the security appliance translates IP address 10.0.0.11 into routable IP address 192.168.6.9.

Access Through the Security Appliance

Cisco.com

Less Secure ← More Secure

Allowed
unless explicitly denied
(NAT and global)

e3 Partnernet
Security Level 50

e2 DMZ
Security Level 30

e4 Intranet
Security Level 70

Internet

e0 outside
Security Level 0

e1 inside
Security Level 100

Less Secure → More Secure

Denied
unless explicitly allowed
(static and access list)

SNPA v4.0—4-11
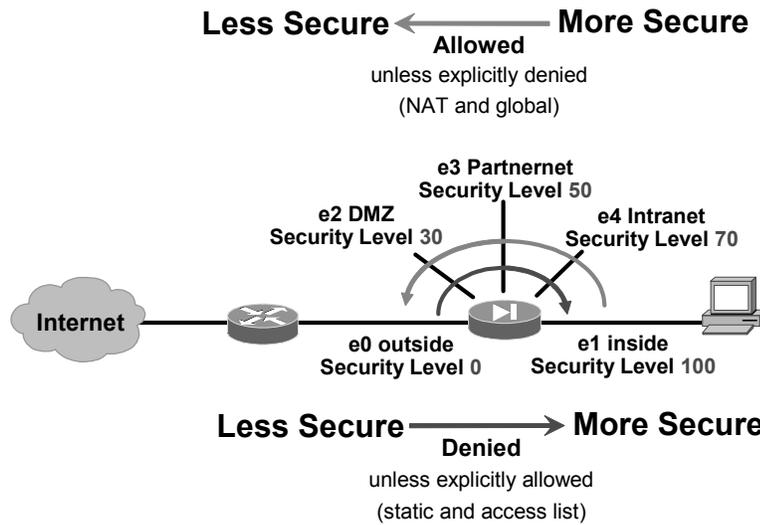
When you are configuring multiple interfaces, remember that the security level designates whether an interface is inside (trusted) or outside (untrusted) relative to another interface. An interface is considered to be inside in relation to another interface if its security level is higher than the security level of the other interface, and an interface is considered to be outside in relation to another interface if its security level is lower than the security level of the other interface.

The primary rule for security levels is that an interface with a higher security level can access an interface with a lower security level. Connections are allowed unless they are explicitly denied. The **nat** and **global** commands work together to enable your network to use any IP addressing scheme and to remain hidden from the external network.

An interface with a lower security level cannot access an interface with a higher security level unless you specifically allow it by implementing **static** and **access list** command pairs.

Inside Address Translation

Cisco.com

NAT

192.168.6.20   10.0.0.4

Internet

Dynamic Translation

Outside global IP address pool 192.168.6.20-254

10.0.0.4

10.0.0.4

Outside Global IP Address

Inside IP Address

Web Server

Static Translation   192.168.6.10 ←→ 10.0.0.11

10.0.0.11
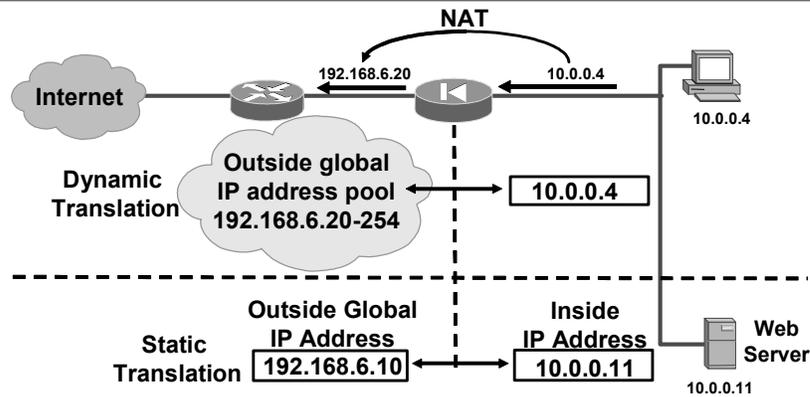
- **Inside NAT translates addresses of hosts on higher security level to a less secure interface:**
  - **Dynamic translation**
  - **Static translation**

SNPA v4.0—4-12

The security appliance supports the following two main types of address translations:

- Dynamic translation: Translates host addresses on more secure interfaces to a range or pool of IP addresses on a less secure interface. This allows internal users to share registered IP addresses and hides internal addresses from view on the public Internet.

- Static translation: Provides a permanent, one-to-one mapping between an IP address on a more secure interface and an IP address on a less secure interface. This allows an inside host to access a less secure host, a server on the Internet, for example, without exposing the actual IP address. Examples of static translation are static NAT and identity NAT.

Dynamic Inside NAT
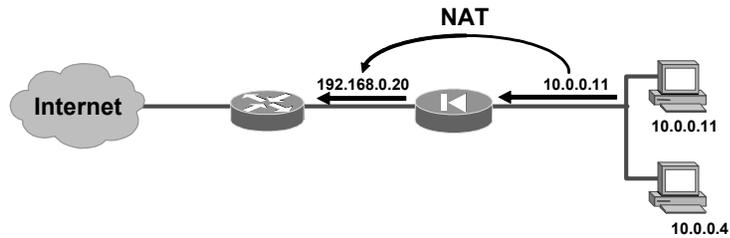
NAT

192.168.0.20   10.0.0.11

Internet

10.0.0.11

10.0.0.4

• **Dynamic translations**

```
fw1(config)# nat (inside) 1 10.0.0.0 255.255.255.0
fw1(config)# global (outside) 1 192.168.0.20-192.168.0.254 netmask 255.255.255.0
```

SNPA v4.0—4-13

Dynamic inside translations are used for local hosts and their outbound connections, and they hide the host address from the Internet. With dynamic translations, you must first define which hosts are eligible for translation with the **nat** command, then define the address pool with the **global** command. The pool for address allocation is chosen on the outgoing interface based on the NAT identifier (NAT ID) selected with the **nat** command.

In the figure, all hosts on the inside network are eligible for translation. The mapped pool of addresses assigned by the **global** command is 192.168.0.20 through 192.168.0.254, enabling up to 235 individual IP addresses.

Two Interfaces with NAT

10.2.0.0 /24

Global Pool
192.168.0.17-32

Internet

192.168.0.0

Global Pool
192.168.0.3-16
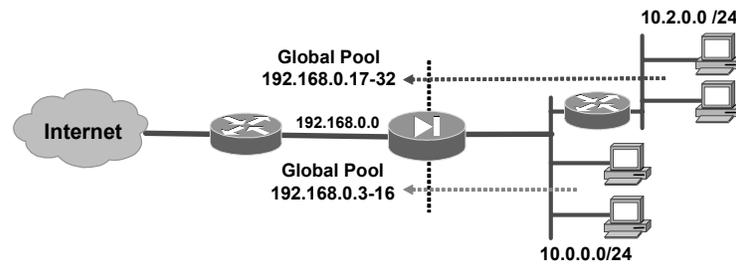
10.0.0.0/24

- **All hosts on the inside networks can start outbound connections.**
- **A separate global pool is used for each internal network.**

```
fw1(config)# nat (inside) 1 10.0.0.0 255.255.255.0
fw1(config)# nat (inside) 2 10.2.0.0 255.255.255.0
fw1(config)# global (outside) 1 192.168.0.3-192.168.0.16 netmask 255.255.255.0
fw1(config)# global (outside) 2 192.168.0.17-192.168.0.32 netmask 255.255.255.0
```

SNPA v4.0—4-14

In the figure, the first **nat** command statement permits all hosts on the 10.0.0.0 network to start outbound connections using IP addresses from a mapped pool. The second **nat** command statement permits all hosts on the 10.2.0.0 network to do the same. The NAT ID in the first **nat** command statement tells the security appliance to translate the 10.0.0.0 addresses to those in the mapped pool containing the same NAT ID. Likewise, the NAT ID in the second **nat** command statement tells the security appliance to translate addresses for hosts on network 10.2.0.0 to the addresses in the mapped pool containing NAT ID 2.

Three Interfaces with NAT

Cisco.com
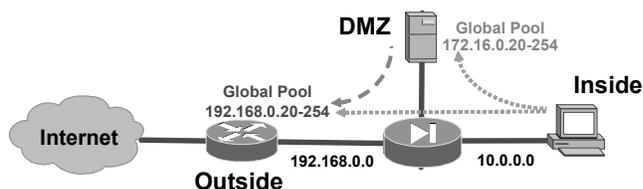
- **Inside users can start outbound connections to both the DMZ and the Internet.**
- **The** nat (dmz) **command enables DMZ services to access the Internet.**
- **The** global (dmz) **command enables inside users to access the DMZ web server.**

```
fw1(config)# nat (inside) 1 10.0.0.0 255.255.255.0
fw1(config)# nat (dmz) 1 172.16.0.0 255.255.255.0
fw1(config)# global (outside) 1 192.168.0.20-192.168.0.254 netmask 255.255.255.0
fw1(config)# global (dmz) 1 172.16.0.20-172.16.0.254 netmask 255.255.255.0
```

SNPA v4.0—4-15

In the figure, the first **nat** command enables hosts on the inside interface, which has a security level of 100, to start connections to hosts on interfaces with lower security levels. In this case, that includes hosts on the outside interface and hosts on the demilitarized zone (DMZ). The second **nat** command enables hosts on the DMZ, which has a security level of 50, to start connections to hosts on interfaces with lower security levels. In this case, that includes only the outside interface.

Because both of the mapped pools and the **nat (inside)** command use a NAT ID of 1, addresses for hosts on the 10.0.0.0 network can be translated to those in either mapped pool. Therefore, when users on the inside interface access hosts on the DMZ, the **global (dmz)** command causes their source addresses to be translated to addresses in the 172.16.0.20−172.16.0.254 range. When they access hosts on the outside, the **global (outside)** command causes their source addresses to be translated to addresses in the 192.168.0.20−192.168.0.254 range.

When users on the DMZ access outside hosts, the **global (outside)** command causes their source addresses to be translated to addresses in the 192.168.0.20−192.168.0.254 range.

Port Address Translation

This topic describes how to configure a Cisco security appliance to take advantage of port address translation (PAT).

Port Address Translation

PAT

192.168.0.20 Port 1024 — 10.0.0.11

Internet

192.168.0.20 Port 1025 — 10.0.0.4

10.0.0.11

10.0.0.4

- **PAT is a combination of an IP address and a source port number.**
- **Many different sessions can be multiplexed over a single global IP address.**
- **Sessions are kept distinct by the use of different port numbers.**

SNPA v4.0—4-17
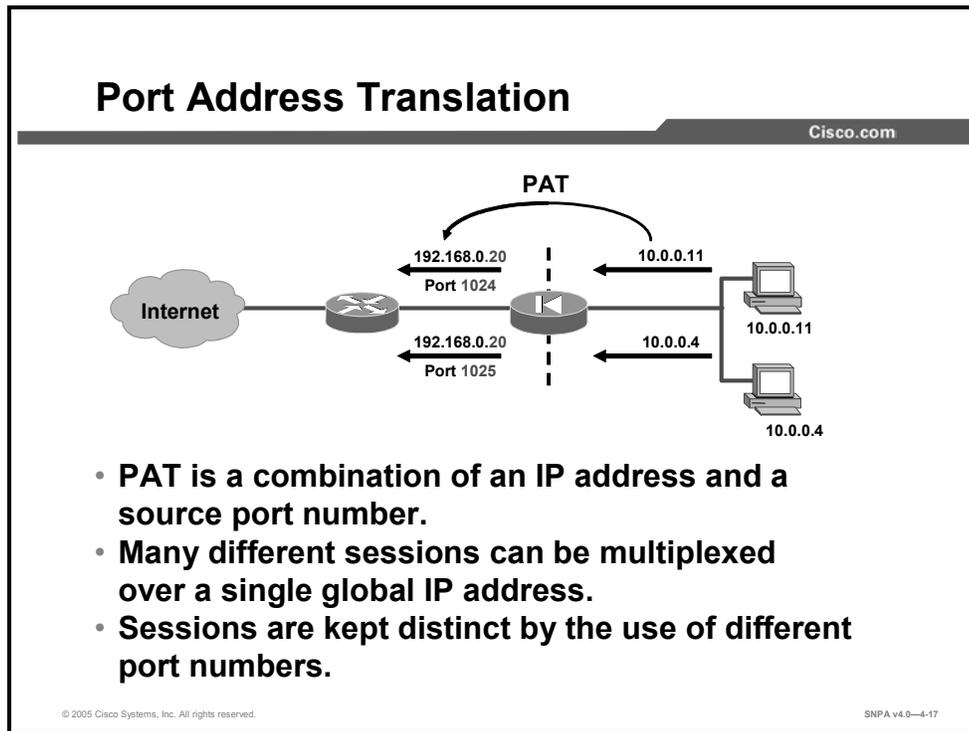
Typically, an enterprise network receives only a small number of addresses from its ISP, whereas the number of hosts is much larger. To resolve this situation, configure PAT, which is an enhancement of NAT.

Using PAT, multiple connections originating from different hosts on the inside networks can be multiplexed by a single mapped IP address. The multiplexing identifier is the source port number. In the figure, the IP addresses of the two hosts on the inside network are translated to a PAT IP address of 192.168.0.20 and source ports 1024 and 1025.

PAT Example

```
fw1(config)# route (outside) 0.0.0.0 0.0.0.0 192.168.0.1
fw1(config)# nat (inside) 1 10.0.0.0 255.255.0.0
fw1(config)# global (outside) 1 192.168.0.3 netmask
   255.255.255.255
```

- **Outside IP addresses are typically registered with InterNIC.**
- **Source addresses of hosts in network 10.0.0.0 are translated to 192.168.0.3 for outgoing access.**
- **A single IP address (192.168.0.3) is assigned to the global pool.**
- **The source port is dynamically changed to a unique number that is greater than 1023.**
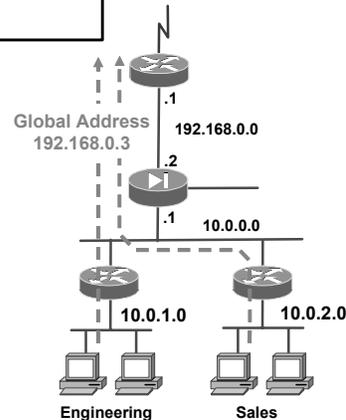
SNPA v4.0—4-18

The security appliance PAT feature expands a company's address pool:

■ One outside IP address is used for up to approximately 64,000 inside hosts.

■ PAT maps TCP and UDP port numbers to a single IP address.

■ PAT hides the inside source addresses by using a single IP address from the security appliance.

■ PAT can be used with NAT.

■ A PAT address can be a virtual address, different from the outside address.

Do not use PAT when running certain multimedia applications through the security appliance. These multimedia applications need access to specific ports and can conflict with port mappings provided by PAT.

In this example of PAT, XYZ Company has only six registered IP addresses. One address is taken by the perimeter router, one by the security appliance, and one by the mapped address.

The example configuration is as follows:

```
ip address inside 10.0.0.1 255.255.255.0
ip address outside 192.168.0.2 255.255.255.0
route outside 0.0.0.0 0.0.0.0 192.168.0.1
```

IP addresses are assigned to the internal and external interfaces. A single registered IP address is put into the mapped pool and is shared by all outgoing access for network 10.0.0.0:

```
nat (inside) 1 10.0.0.0 255.255.0.0
global (outside) 1 192.168.0.3 netmask 255.255.255.255
```

PAT Using Outside Interface Address

```
fw1(configs)# interface ethernet0
fw1(configs-if)# ip address inside 10.0.0.1 255.255.255.0
fw1(configs-if)# ip address outside dhcp
fw1(configs)# nat (inside) 1 10.0.0.0 255.255.0.0
fw1(config)# global (outside) 1 interface
```

- **The outside interface is configured as a DHCP client.**

- **The interface option of the** global **command enables use of a DHCP address as the PAT address.**

- **The source addresses of hosts in network 10.0.0.0 are translated into a DHCP address for outgoing access, in this case, 192.168.0.2.**

- **The source port is changed to a unique number greater than 1023.**

Global DHCP Address (192.168.0.2)

192.168.0.0

.1

.2

.1 **10.0.0.0**

10.0.1.0   **10.0.2.0**

Engineering   **Sales**
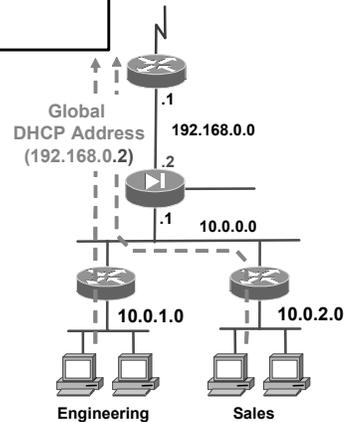
SNPA v4.0—4-19

You can use the IP address of the outside interface as the PAT address by using the interface option of the **global** command. This is important when using Dynamic Host Configuration Protocol (DHCP) because it allows the DHCP-retrieved address to be used for PAT.

In the figure, source addresses for hosts on network 10.0.0.0 are translated to the DHCP-retrieved IP address of 192.168.0.2 for outgoing access, and the source port is changed to a unique number greater than 1023.

Mapping Subnets to PAT Addresses

```
fw1(config)# nat (inside) 1 10.0.1.0 255.255.255.0
fw1(config)# nat (inside) 2 10.0.2.0 255.255.255.0
fw1(config)# global (outside) 1 192.168.0.8 netmask
    255.255.255.255
fw1(config)# global (outside) 2 192.168.0.9 netmask
    255.255.255.255
```

- **Each internal subnet is mapped to a different PAT address.**
- **Source addresses of hosts in network 10.0.1.0 are translated to 192.168.0.8 for outgoing access.**
- **Source addresses of hosts in network 10.0.2.0 are translated to 192.168.0.9 for outgoing access.**
- **The source port is changed to a unique number greater than 1023.**

192 .168.0.9
192 .168.0.8
.1
192.168.0.0
.2
.1 10.0.0.0
10.0.1.0   10.0.2.0
Engineering   Sales
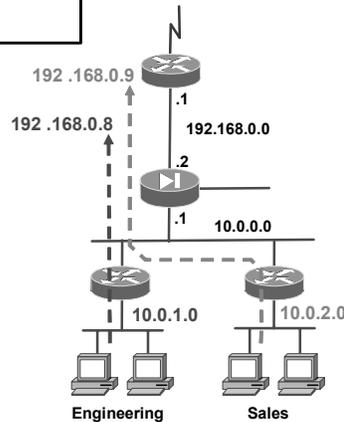
SNPA v4.0—4-20

With Cisco PIX Firewall Security Appliance Software v5.2 and higher, you can specify multiple PATs to track use among different subnets. In the figure, network 10.0.1.0 and network 10.0.2.0 are mapped to different PAT addresses. This is done by using a separate **nat** and **global** command pair for each network. Outbound sessions from hosts on internal network 10.0.1.0 will seem to originate from address 192.168.0.8, and outbound sessions from hosts on internal network 10.0.2.0 will seem to originate from address 192.168.0.9.

Backing Up PAT Addresses by Using Multiple PATs

```
fw1(config)# nat (inside) 1 10.0.0.0 255.255.252.0
fw1(config)# global (outside) 1 192.168.0.8 netmask
   255.255.255.255
fw1(config)# global (outside) 1 192.168.0.9 netmask
   255.255.255.255
```

192 .168.0.9

.1

192 .168.0.8

192.168.0.0

.2

.1   10.0.0.0

- **Source addresses of hosts in network 10.0.1.0 are translated to 192.168.0.8 for outgoing access.**

- **Address 192.168.0.9 will be used only when the port pool from 192.168.0.8 is at maximum capacity.**

10.0.1.0   10.0.2.0

Engineering   Sales
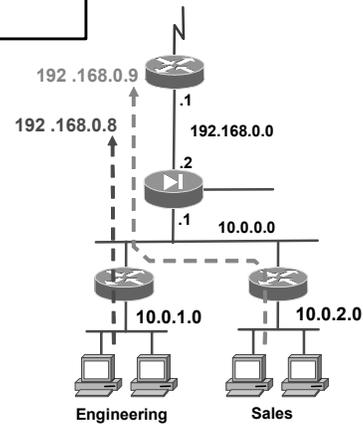
SNPA v4.0—4-21

With PIX Firewall Security Appliance Software v5.2 and higher, you also can back up your PAT address by having multiple global configurations with the same NAT ID.

In the figure, address 192.168.0.9 will be used for all outbound connections from network 10.0.0.0/22 when the port pool from 192.168.0.8 is at maximum capacity.

Augmenting a Global Pool with PAT

```
fw1(config)# nat (inside) 1 10.0.0.0 255.255.0.0
fw1(config)# global (outside) 1 192.168.0.20-192.168.0.253 netmask
   255.255.255.0
fw1(config)# global (outside) 1 192.168.0.254 netmask
   255.255.255.255
```

NAT
192 .168.0.20
PAT
192 .168.0.254

192.168.0.0

10.0.0.0

- **When hosts on the 10.0.0.0 network access the outside network through the security appliance, they are assigned public addresses from the 192.168.0.20–192.168.0.253 range.**
- **When the addresses from the global pool are exhausted, PAT begins with the next available IP address, in this case, 192.168.0.254.**

10.0.1.0   10.0.2.0

Engineering   Sales
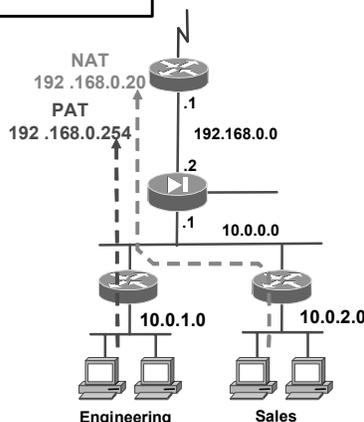
SNPA v4.0—4-22

You can augment a pool of mapped addresses with PAT. When all IP addresses from the mapped pool are in use, the security appliance begins PAT, using the single IP address shown in the second **global** command.

In the figure, hosts on the 10.0.0.0/16 internal network are assigned addresses from the mapped pool 192.168.0.20 through 192.168.0.253 as they initiate outbound connections. When the addresses from the mapped pool are exhausted, packets from all hosts on network 10.0.0.0/16 seem to originate from 192.168.0.254.

Identity NAT

DMZ
Internet
Server
192.168.0.9

192.168.0.9

10.0.0.15

Internet

Outside

Inside
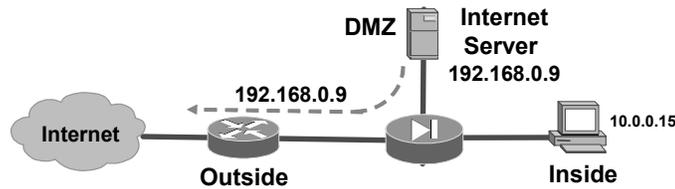
With NAT control enabled:

- **All packets traversing a security appliance require a translation rule.**
- **Identity NAT is used to create a transparent mapping.**
- **IP addresses on the high security interface translate to themselves on *all* lower security interfaces.**

SNPA v4.0—4-23

With NAT control enabled, all packets traversing the security appliance require a translation rule. The **nat 0** command, also know as identity NAT, enables you to map IP addresses transparently so that inside IP addresses are visible on the outside without address translation. IP addresses on the higher security interface translate to themselves on *all* lower security interfaces. Use this feature when you have Internet Network Information Center (InterNIC)-registered IP addresses on your inside network that you want accessible on the outside network. Use of the **nat 0** command depends on your security policy. If your policy allows internal clients to have their IP addresses exposed to the Internet, then use the **nat 0** command, identity NAT, to provide that service.

Your network security policy may dictate that the IP addresses of most, but not all, hosts need to be protected by employing NAT. With NAT control disabled, which is the default, only hosts whose addresses must be protected need an address translation rule to be configured for them. If a traversing packet matches a translation rule, the address is translated. If there are no NAT rules that match the traversing packet, NAT is not applied. Disabling NAT control may obviate the need to configure identity NATs in your network. The administrator still needs to add an access control list (ACL) to allow users on the outside to initiate a connection with an inside devices via their real (nontranslated) IP address.

Identity NAT: *nat 0* Command

Cisco.com

DMZ
192.168.0.9

Internet
Server

192.168.0.9

Internet

Inside
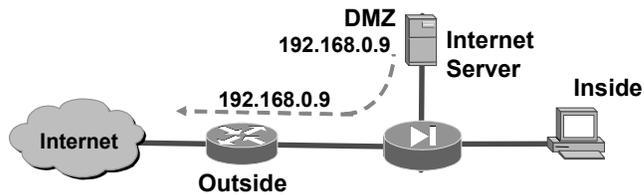
Outside

- **NAT 0 ensures that the Internet server is translated to its own address on the outside.**
- **Security levels remain in effect with NAT 0.**

```
fw1(config)# nat (dmz) 0 192.168.0.9 255.255.255.255
```

SNPA v4.0—4-24

In the figure shown, the address 192.168.0.9 is not translated. When you enter **nat (DMZ) 0 192.168.0.9 255.255.255.255**, the security appliance displays a message that informs you that NAT 0 192.168.0.9 will be nontranslated. It is important to note that NAT 0 enables the Internet server address to be visible on the outside interface.

The administrator also needs to add a static in combination with an ACL to allow users on the outside to connect with the Internet server.

static Command

This topic describes how to configure a permanent mapping between two IP addresses through a Cisco security appliance.

Global NAT and Static NAT

Global NAT
- **For dynamic NAT and PAT address assignments**
- **Inside end user receives an address from a pool of available addresses**
- **Used mostly for outbound end-user connections**

Static
- **For NAT "permanent" address assignments**
- **Used mostly for server connections**

SNPA v4.0—4-26
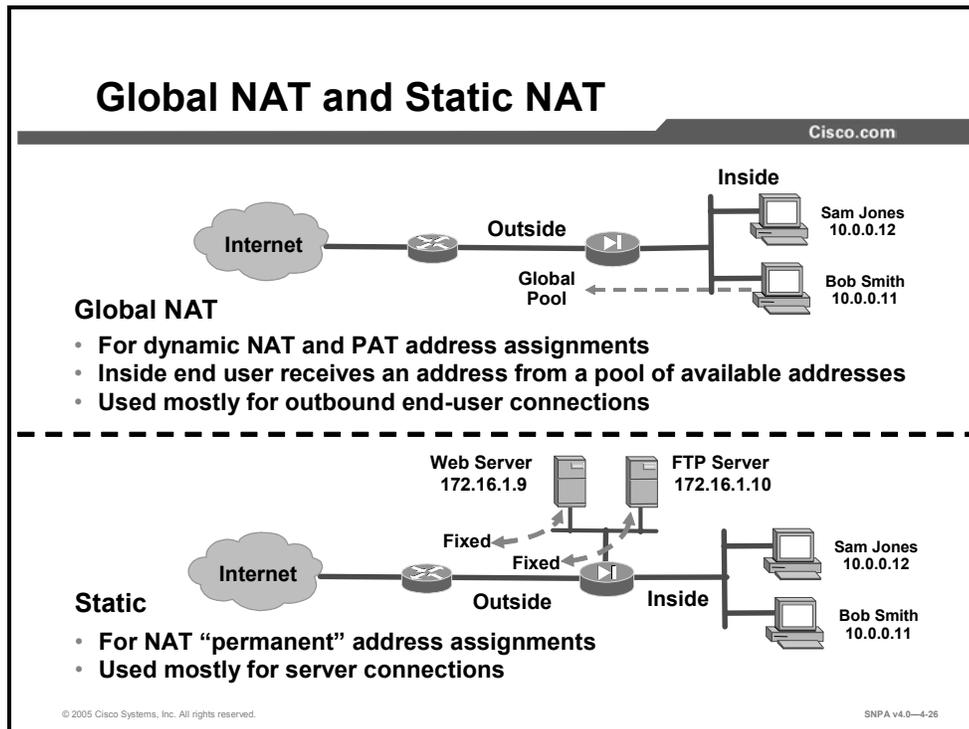
Global NAT configurations are typically used to assign a dynamic address to the end user as they attempt to make a connection to a resource on the outside network. The source IP address is translated to either a mapped NAT or PAT address. The address is assigned dynamically. Each time an end user attempts an outside connection, a different translated address could be assigned to the end user. In the reverse direction, users from the outside network cannot reliably initiate a connection to a host that uses a dynamic address. Not only can you not predict the dynamic IP address of the host, but the security appliance does not create a translation unless the local host is the initiator.

Static NAT creates a fixed translation of local addresses into mapped addresses. With dynamic NAT and PAT, each time an end user attempts an outside connection, a different translated address could be assigned. With static NAT, the mapped address is the same for each consecutive connection. A persistent translation rule exists. Static NAT allows hosts on the outside network to initiate traffic to a local host (if there is an ACL that allows it).

Use static translations when you want an inside server to always appear with a fixed address on the security appliance outside network. Static translations are used to map an inside host address to a static, outside, mapped address:

- Use the **static** command for outbound connections to ensure that packets leaving an inside host are always mapped to a specific IP address (for example, an inside DNS or Simple Mail Transfer Protocol [SMTP] host).

- Use the **static** command for outbound connections that must be mapped to the same IP address.

The following information can help you determine when to use static translations in the security appliance:

- Do not create static translations with overlapping IP addresses. Each IP address should be unique.

- Static commands take precedence over **nat** and **global** command pairs.

- If a mapped IP address is used for PAT, do not use the same mapped IP address for a static translation.

static Command: Parameters

Cisco.com
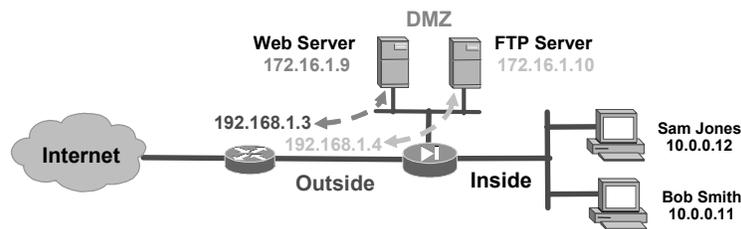
Interfaces

- **Real interface – DMZ**
- **Mapped interface – Outside**

IP Addresses

- **Real IP address – 172.16.1.9**
- **Mapped IP address – 192.168.1.3**

SNPA v4.0—4-27

To configure a static translation, the administrator needs to know a minimum of four parameters. They must know between which two interfaces the translation is performed. The two interfaces are defined as the real and the mapped interface. Next, they need to know the two IP addresses, the real IP address and the translated, or mapped, address. In the example in the figure, the translation is performed between the outside and DMZ interfaces. The DMZ is the real interface; the outside interface is the mapped interface. An IP address of 172.16.1.9 is translated to 192.168.1.3. The 172.16.1.9 IP address is the real address, and 192.168.1.3 is the mapped, or translated, IP address.

static Command: Web Server
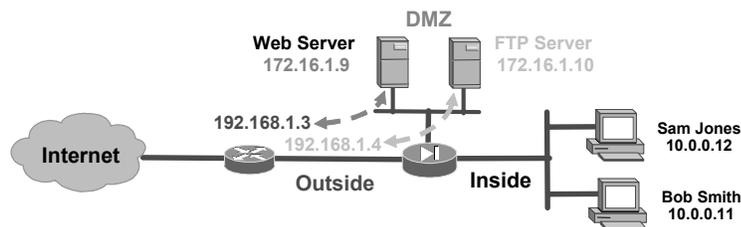
DMZ

Web Server
172.16.1.9

FTP Server
172.16.1.10

192.168.1.3

Internet

192.168.1.4

Outside

Inside

Sam Jones
10.0.0.12

Bob Smith
10.0.0.11

pixfirewall(config)#

```
static (real_interface,mapped_interface) {mapped_address
 | interface} real_address [netmask mask]
```

- **Packets sent to 192.168.1.3 on the outside are translated to 172.16.1.9 on the DMZ.**
- **Permanently maps the Web server IP address.**

```
fw1(config)# static (dmz,outside) 192.168.1.3 172.16.1.9 netmask 255.255.255.255
```

SNPA v4.0—4-28

The **static** command creates a permanent mapping between a real IP address and a mapped IP address. For outbound connections, use the **static** command to specify a mapped address to which the actual or real IP address of a local server will be translated. In the example in the figure, the administrator configured a static translation of the web server's IP address. In the example, the translation takes place between two interfaces, the DMZ interface and the outside interface. There are two IP addresses, the real IP address and the mapped, or translated, IP address. When configuring a **static** command, the interfaces are defined first. The real interface, the DMZ, is entered first. The mapped interface, the outside interface, is entered second. After you define the interfaces, you need to configure the IP addresses. The mapped IP address, 192.168.1.3, is entered first. The real address, 172.16.1.9, is entered second. In the figure, when a packet from the web server traverses the security appliance between the DMZ and the outside interfaces, the web server source IP address of 172.16.1.9 is translated to 192.168.1.3.

The syntax for the **static** command is as follows:

```
static (real_interface,mapped_interface) {mapped_address |
interface} real_address [netmask mask]
```

static Command

real_interface	The network interface name, usually the higher security level interface, in which case the translation is applied to the higher security level address.
mapped_interface	Name of the network interface, as specified by the **nameif** command, where the *real_address* argument is translated into the *mapped-address* argument.
mapped_address	The address into which the real address is translated.
interface	Specifies the interface IP address for the global address. Use this keyword if you want to use the interface address but the address is dynamically assigned using DHCP.
real_address	The address to be mapped.
mask	The network mask that applies to both the mapped address and the real address.

Static NATs take precedence over **nat** and **global** command pairs. Use the **show run static** command to view static statements in the configuration.

static Command: FTP Server
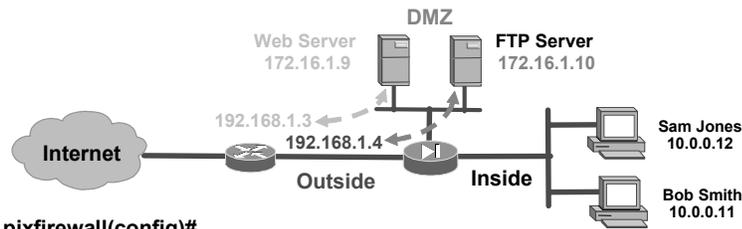
DMZ

Web Server
172.16.1.9

FTP Server
172.16.1.10

192.168.1.3

Internet

192.168.1.4

Outside

Inside

Sam Jones
10.0.0.12

Bob Smith
10.0.0.11

pixfirewall(config)#

```
static (real_interface,mapped_interface)
  {mapped_address | interface} real_address [netmask
  mask]
```

- **Packets sent to 192.168.1.4 on the outside are translated to 172.16.1.10 on the DMZ.**

- **Permanently maps the FTP server IP address.**

```
fw1(config)# static (dmz,outside) 192.168.1.4 172.16.1.10 netmask 255.255.255.255
```

SNPA v4.0—4-29

In the example in the figure, the administrator wants the IP address of the FTP server on the DMZ to be "permanently" translated or mapped to a different IP address on the outside interface. The two interfaces are DMZ and outside. The two IP addresses are 192.168.1.4 and 172.16.1.10.

Net Static
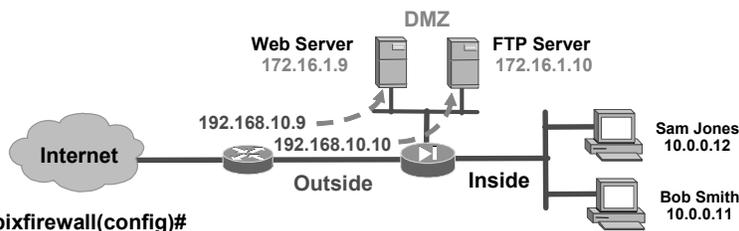
DMZ

Web Server
172.16.1.9

FTP Server
172.16.1.10

192.168.10.9

Internet

192.168.10.10

Outside

Inside

Sam Jones
10.0.0.12

Bob Smith
10.0.0.11

pixfirewall(config)#

```
static (real_interface,mapped_interface)
  {mapped_address | interface} real_address [netmask
  mask]
```

- **Recommended when you want to translate multiple addresses with a single command**
- **Host address on 172.16.1.0 subnet is translated to host address on 192.168.10.0 subnet**

```
fw1(config)# static (dmz,outside) 192.168.10.0 172.16.1.0 netmask 255.255.255.0
```

SNPA v4.0—4-30

You can also use the **static** command to permanently map host addresses on one subnet to a subnet that is on a lower-security interface, also known as a net static. It is recommended when you want to translate multiple hosts on one subnet to another using a single command. In the figure, the administrator wants the server addresses on the DMZ to be translated to a subnet on the outside interface. To accomplish this, the administrator configures a **static** command with two subnets rather than two host addresses. Any packet sourced from a server address on subnet 172.16.1.0/24 on the DMZ is translated to a host address on the 192.168.10.0/24 subnet on the outside interface.

Static PAT: Port Redirection

Cisco.com
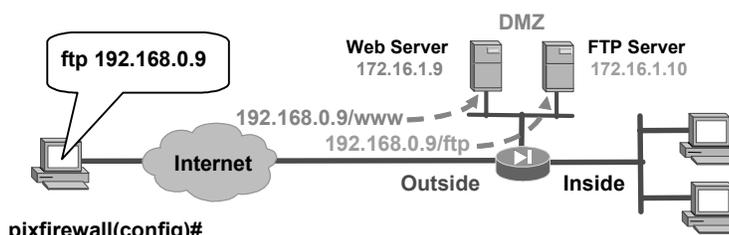
DMZ

ftp 192.168.0.9

Web Server
172.16.1.9

FTP Server
172.16.1.10

192.168.0.9/www

192.168.0.9/ftp

Internet

Outside   Inside

```
pixfirewall(config)#
```

```
static [(real_interface, mapped_interface)] {tcp |
  udp} {mapped_ip | interface} mapped_port
  {real_ip real_port [netmask mask]
```

- **Used to create a permanent translation between a mapped
  IP address and port number to a specific real IP address
  and port number**
  – **192.168.0.9/www redirected to 172.16.1.9/www**
  – **192.168.0.9/ftp redirected to 172.16.1.10/ftp**

SNPA v4.0—4-31

The security appliance provides static PAT capability. This enables outside users to connect to a particular IP address and port. The security appliance redirects traffic to the appropriate inside server and port number. This capability can be used to send multiple inbound TCP or UDP services to different internal hosts through a single global address. The shared address can be a unique address or a shared outbound PAT address, or it can be a shared with the external interface. If the keyword **tcp** or **udp** is specified in the **static** command, a static UDP or TCP port redirection is configured. If the key word **interface** is specified, the outside interface address is presumed to be the mapped IP address. For example, if you want to provide a single address for global users to access the FTP and web servers, but these are all actually different servers on the local network, you can specify static statements for:

■ Mapped FTP IP address to real IP address

  ▪ 192.168.0.9/www to 172.16.1.9/www

■ Mapped Hypertext Transfer Protocol (HTTP) IP address to real IP address

  ▪ 192.168.0.9/ftp to 172.16.1.9/ftp

In the example in the figure, if a web packet is sent to 192.168.0.9, it is redirected to the web server at IP address 172.16.1.9. If an FTP packet is sent to 192.168.0.9, it is redirected to the FTP server at IP address 172.16.1.10.

You also can use this feature to translate a well-known port to a lesser-known port or vice versa. For example, if the inside web server uses port 80, you can allow outside users to connect to port 8080, then translate them to the correct port. Similarly, if you want to provide extra security, you can tell your web users to connect to lesser-known port 6785, then translate them to port 80 on the local network.

The syntax for the **static** command is as follows:

```
static (real_interface, mapped_interface) {tcp | udp}
{mapped_ip | interface} mapped_port {real_ip real_port
[netmask mask]
```

static Command

real_interface	The network interface name, usually the higher security level interface, in which case the translation is applied to the higher security level address.
mapped_interface	Name of the network interface, as specified by the **nameif** command, where the *real_ip* argument are translated into the *mapped_ip* argument.
tcp	Specifies a TCP port.
udp	Specifies a UDP port.
mapped_ip	Specifies the global IP address(es) to which you want to translate the local address(es). You can map a single mapped address to a single local address or a range of mapped addresses to a range of local addresses. This address cannot be used as a dynamic PAT IP address in the **mapped** command unless you use static PAT, in which case the two addresses can be the same.
interface	Specifies the interface IP address for the global address. Use this keyword if you want to use the interface address, but the address is dynamically assigned using DHCP.
mapped_port	Specifies the mapped TCP or UDP port. You can specify ports by either a literal name or a number in the range of 0 through 65535.
real_ip	Specifies the addresses to translate. You can map a single local address to a single real address or map a range of local addresses to a range of real addresses.
real_port	Specifies the real TCP or UDP port. You can specify ports by either a literal name or a number in the range of 0 through 65535.
mask	The network mask that applies to both the mapped addresses and the real addresses.

static pat Command

DMZ

FTP1 Server 172.16.1.9 **FTP2 Server** 172.16.1.10

ftp 192.168.0.9

192.168.0.9/FTP
192.168.0.9/2121

Internet

Outside **Inside**
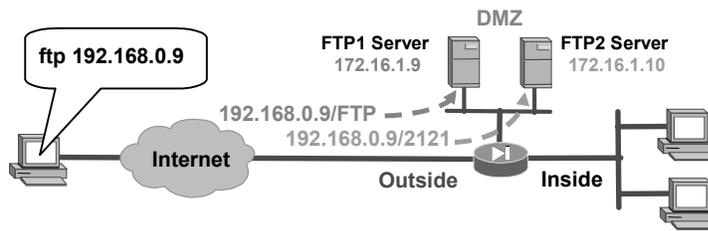
- **Packet sent to 192.168.0.9/FTP translated by security appliance to 172.16.1.9 (first FTP server)**
- **Packet sent to 192.168.0.9/2121 translated by security appliance to 172.16.1.10 (second FTP server)**

```
fw1(config)# static (dmz,outside) tcp 192.168.0.9 ftp 172.16.1.9 ftp netmask
  255.255.255.255
fw1(config)# static (dmz,outside) tcp 192.168.0.9 2121 172.16.1.10 ftp netmask
  255.255.255.255
```

SNPA v4.0—4-32

Note that after FTP, port 21, is used on the PAT address, it can't be redirected to a different inside host, a second FTP server. To access a second FTP server, the administrator would have outside clients use a different port number, for example, port 2121. The administrator could configure the security appliance to redirect port 2121 to the second inside FTP server. In the figure, an external user directs an FTP request to the security appliance address 192.168.0.9. The security appliance redirects the request to the DMZ FTP server at IP address 172.16.1.9. To access the second FTP server, the external user directs an FTP request to the security appliance address 192.168.0.9 port 2121. The security appliance redirects the request to the second FTP server at IP address 172.16.1.10. (To enable the external user to access the FTP server, an ACL would also have to be present in the configuration.)

TCP Intercept and Connection Limits

This topic describes the TCP Intercept feature and how to set embryonic, TCP, and UDP connection limits in Cisco security appliances.

Connection Limits

Administrator can set connection limits:

- *Emb_lin* **– Maximum number of embryonic connections per host. An embryonic connection is a connection request that has not completed a TCP three-way handshake between the source and the destination.**

- *TCP_max_conns* **– Maximum number of simultaneous TCP connections that each real IP host is allowed to use. Idle connections are closed after the time specified by the** timeout conn **command.**

- *udp_max_conns* **– Maximum number of simultaneous UDP connections that each real IP host is allowed to use.**

SNPA v4.0—4-34

Protection against various denial of service (DoS) attacks has increased through newer versions of security appliance operating systems. Beginning in Cisco PIX Firewall Security Appliance Software v5.2, TCP Intercept provided for proxy resets of sessions without any knowledge or interference from the destination station. Release 6.2 introduced SYN cookies, a proxy verification tool that the security appliance operating system uses to validate a new session.

tcp_max_conns argument in a static or nat command enables the administrator to limit the number of connections a host is permitted to use. Cisco PIX and ASA Security Appliance Software v7.0 introduced UDP maximum connections argument. *udp_max_conns* argument in a static or anat command enables the administrator to limit the number of UDP connections that a host is permitted to use. These parameters are covered in greater detail later in this lesson.

TCP Three-Way Handshake

Normal

SYN, SRC: 172.26.26.45, DST: 10.0.0.2

SYN-ACK

ACK

Target 10.0.0.2

172.26.26.45

DoS Attack

Internet

SYN, SRC: 172.16.16.20 DST: 10.0.0.3
SYN, SRC: 172.16.16.20 DST: 10.0.0.3
SYN, SRC: 172.16.16.20 DST: 10.0.0.3

Target 10.0.0.3

172.26.26.46

Embryonic Connection

SYN-ACK
SYN-ACK
SYN-ACK

?
?
?

Spoofed Host 172.16.16.20
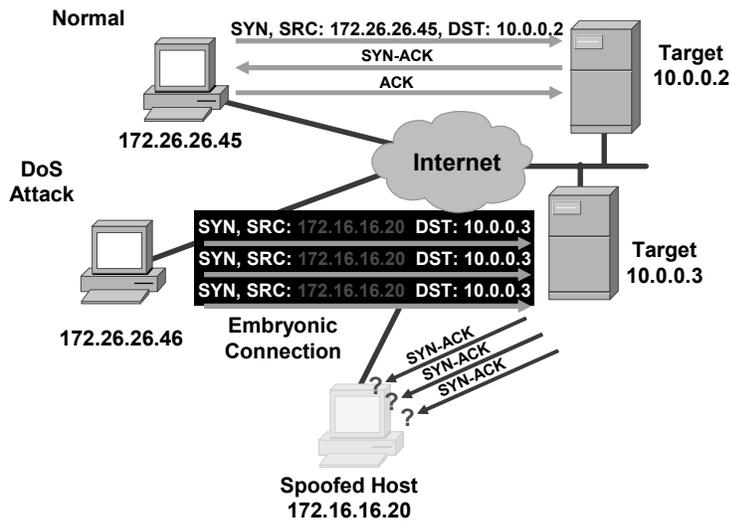
SNPA v4.0—4-35

SYN flood attacks, also known as TCP flood attacks and half-open, or embryonic, connections attacks, are common DoS attacks perpetrated against IP servers. The attacker spoofs a nonexistent source IP address and floods the target with SYN packets that are pretending to come from the spoofed host. SYN packets to a host are the first step in the three-way handshake of a TCP-type connection; therefore, the target responds as expected with SYN-ACK packets destined for the spoofed host or hosts. Because these SYN-ACK packets are sent to hosts that do not exist, the target sits and waits for the corresponding ACK packets that never show up. This causes the target to overflow its port buffer with embryonic connections and to stop responding to legitimate requests.

TCP Intercept
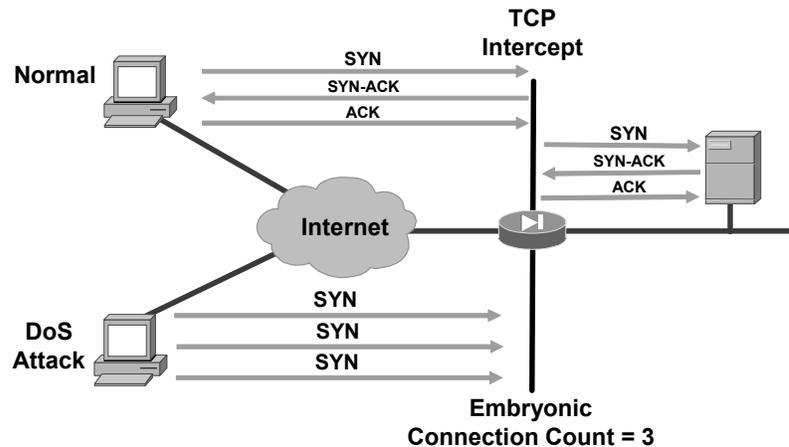
With the TCP Intercept feature in releases 5.2 and higher, after the optional embryonic connection limit is reached and until the embryonic connection count falls below this threshold, every SYN bound for the affected server is intercepted. For each SYN, the security appliance responds on behalf of the server with an empty SYN-ACK segment. The security appliance retains pertinent state information, drops the packet, and waits for the client's acknowledgment. If the ACK is received, a copy of the client's SYN segment is sent to the server, and the TCP three-way handshake is performed between the security appliance and the server. Only if this three-way handshake completes will the connection be allowed to resume as normal.

SYN Cookies

TCP Intercept

Normal

SYN

SYN-ACK (Cookie)

ACK (Cookie)

SYN

SYN-ACK

ACK

Internet
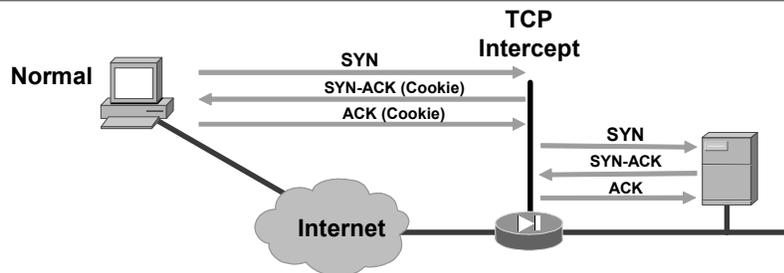
The security appliance responds to the SYN itself, which includes a cookie in the TCP header of the SYN-ACK. The security appliance keeps no state information.

- **The cookie is a hash of parts of the TCP header and a secret key.**
- **A legitimate client completes the handshake by sending the ACK back with the cookie.**
- **If the cookie is authentic, the security appliance proxies the TCP session.**

SNPA v4.0—4-37

In release 6.2, the SYN cookies feature was introduced. This feature is a less CPU-intensive method of checking the validity of incoming TCP sessions. SYN cookies are an implementation of TCP in which a security appliance responds to a TCP SYN request with a cookie. In the original TCP implementation, when a security appliance received a SYN packet, it responded with a SYN-ACK and entered the half-open state to wait for the ACK that would complete the handshake. Too many half-open connections can result in buffer issues.

With SYN cookies, after the embryonic connection limit is reached, the security appliance receives a SYN packet and responds with a SYN-ACK packet in which the ACK sequence number is calculated from the source address, source port, source sequence number, destination address, destination port, and a secret seed. Then the security appliance releases all state information. If an ACK returns from the client, the security appliance can recalculate it to determine if it is a response to a previous SYN-ACK. If so, the security appliance can attempt to open a connection to the server. In this way, both the security appliance and the server avoid managing a batch of potentially useless embryonic connections. SYN cookies is more scalable in terms of performance. This feature replaces TCP Intercept.

Embryonic Connection Limit

firewall (config)#

```
static (real_ifc,mapped_ifc) {mapped_ip | interface}
  {real_ip [netmask mask] | access-list
  access_list_name} [dns] [norandomseq] [[tcp]
  [max_conns [emb_lim]] [udp udp_max_conns]
```

firewall (config)#

```
nat (local_interface) nat_id local_ip [mask] [dns]
  [outside] [[tcp] tcp_max_conns [emb_limit]
  [norandomseq]]] [udp udp_max_conns]
```

- **Setting the embryonic connections (*emb_lim*) enables TCP proxying using either TCP Intercept or SYN cookies.**
  - **A value of 0 disables protection (default).**
  - **When the embryonic connection limit is exceeded, all connections are proxied.**

```
fw1(config)# nat (inside) 1 0 0 0 25
fw1(config)# static (inside,outside) 192.168.0.11
  172.16.0.2 0 25
```

SNPA v4.0—4-38

To protect internal hosts against DoS attacks, limit the number of embryonic connections that are allowed to the server. To accomplish this, set the embryonic connections limit, or threshold, to a non-zero number. (A value of zero disables embryonic connections protection.) The embryonic connections threshold is configurable using either the **static** or the **nat** command. In the example in the figure, both the **nat** command and the **static** command set the embryonic connections threshold to 25.

The syntax used in the **static** command for enabling TCP Intercept is as follows:

```
static (real_ifc,mapped_ifc) {mapped_ip | interface} {real_ip
[netmask mask]} | {access-list access_list_name} [dns]
[norandomseq [nailed]] [[tcp] max_conns [emb_lim]] [udp
udp_max_conns]
static (real_ifc,mapped_ifc) {tcp | udp} {mapped_ip |
interface} mapped_port {real_ip real_port [netmask mask]} |
{access-list access_list_name} [dns] [norandomseq [nailed]]
[[tcp] max_conns [emb_lim]] [udp udp_max_conns]
```

static Command for Enabling TCP Intercept

real_ifc	(Optional) Name of the network interface, as specified by the **nameif** command, at which the hosts or networks that are designated by the specified real IP address or sources in the ACL are accessed.
mapped_ifc	(Optional) . Name of the network interface, as specified by the **nameif** command, where the *real_ip* argument is translated into the mapped_ip argument.
mapped_ip	Masquerade address of the real IP address or of the source address in the ACL.
interface	Address taken from the mapped address.
real_ip	Address as configured at the actual host.
netmask *mask*	Specifies the IP netmask to apply to the real IP address.
access-list	Allows you to identify local traffic for network address translation (NAT) by specifying the local and destination addresses (or ports).
access_list_name	Specifies the ACL name.
dns	(Optional) Rewrites the local address in DNS replies to the global address. Rewrite the A record, or address record, in DNS replies that match this static. For DNS replies traversing from a mapped interface to a real interface, the A record is rewritten from the mapped value to the real value. Inversely, for DNS replies traversing from a real interface to a mapped interface, the A record is rewritten from the real value to the mapped value.
norandomseq	(Optional) Disables TCP initial sequence number randomization protection.
tcp	(Optional) Specifies that maximum TCP connections and embryonic limits are set for TCP.
max_conns	Maximum number of simultaneous TCP connections that each real IP variable host is allowed to use. Idle connections are closed after the time specified by the **timeout conn** command.
emb_lim	(Optional) Maximum number of embryonic connections per host. An embryonic connection is a connection request that has not completed a TCP three-way handshake between the source and destination.
udp	(Optional) Specifies that a maximum number of UDP connection parameters are configured. Or specifies UDP static PAT.
udp_max_conns	(Optional) Used with the **udp** keyword to set the maximum number of simultaneous UDP connections that the local IP hosts each are allowed to use.

Use the **nat** command to protect external hosts against DoS attacks and to limit the number of embryonic connections from the internal host. Use the *emb_limit* argument to set the maximum number of embryonic connections that are allowed.

The syntax used in the **nat** command for enabling the TCP Intercept is as follows:

```
nat (local_interface) nat_id local_ip [mask [dns] [outside]
[[tcp] max_conns [emb_limit] [norandomseq]]] [udp
udp_max_conns]
nat (local_interface) nat_id access-list access_list_name
[dns] [outside] [[tcp] max_conns [emb_limit] [norandomseq]]]
[udp udp_max_conns]
```

nat Command

local_interface	Name of the network interface as specified by the **nameif** command through which the hosts or networks that are designated by the internal network IP address are accessed.
nat_id	ID of the group of host or networks.
local_ip	Internal network IP address to be translated.
mask	(Optional) IP netmask to apply to the internal network IP address.
dns	(Optional) Specifies to use the created translation to rewrite the DNS address record.
outside	(Optional) Specifies that the **nat** command apply to the outside interface address.
tcp	(Optional) Specifies that the maximum TCP connections and the embryonic limit are set for the TCP protocol.
max_conns	(Optional) Maximum number of simultaneous connections that the internal network IP hosts allow. Idle connections are closed after the time that is specified by the **timeout connection** command.
emb_limit	(Optional) Maximum number of embryonic connections per host.
norandomseq	(Optional) Disables TCP initial sequence number randomization protection.
udp	(Optional) Specifies a maximum number of UDP connection parameters that can be configured.
udp_max_conns	(Optional) Sets the maximum number of simultaneous UDP connections that the internal network IP hosts are each allowed to use. Idle connections are closed after the time that is specified by the **timeout connection** command.

UDP Maximum Connection Limit

firewall (config)#

```
static (real_ifc,mapped_ifc) {mapped_ip | interface}
  {real_ip [netmask mask]} | {access-list
  access_list_name} [dns] [[tcp] [max_conns [emb_lim]]
  [norandomseq] ]] [udp udp_max_conns]
```

firewall (config)#

```
nat {local_interface} nat_id local_ip [mask [dns]
  [outside] [[tcp] tcp_max_conns [emb_limit]
  [norandomseq]]] [udp udp_max_conns]
```

- **Maximum number of simultaneous UDP connections that the local IP hosts are allowed.**
  - **A value of 0 disables protection (default).**
  - **Idle connections are closed after the time specified in the** udp timeout **command.**

```
fw1(config)# nat (inside) 1 0.0.0.0 0.0.0.0 200 25
fw1(config)# static (inside,outside) 192.168.0.11
  172.16.0.2 0 0 udp 100
```

SNPA v4.0—4-39

Use *udp_max_conns* to set the maximum number of simultaneous UDP connections that the internal network IP hosts are each allowed to use. Idle connections are closed after the time that is specified by the **timeout udp** command. The default is 2 minutes.

Use *tcp_max_conns* to set the maximum number of simultaneous TCP connections that the internal network IP hosts are each allowed to use. Idle connections are closed after the time that is specified by the **timeout conn** command. The default is 1 hour. In the NAT example in the figure, the maximum number of TCP connections is set to 200 and the embryonic limit is set to 25.

In both the **nat** and **static** commands, you can set the maximum number of simultaneous UDP connections even when the maximum number of simultaneous TCP connections is not set, by using the keyword **udp**. This allows the two limits to be exclusively configured. In the example in the figure, the static connection between 192.168.0.11 and 172.16.0.2 is limited to a maximum of 100 UDP connections.

The administrator can also set the TCP, UDP, and embryonic limits on a per-flow basis by using the **set connection** command in a policy map.

Connections and Translations

This topic describes how connections and translations are different and how to verify them in a Cisco security appliance.

Connections Versus Translations
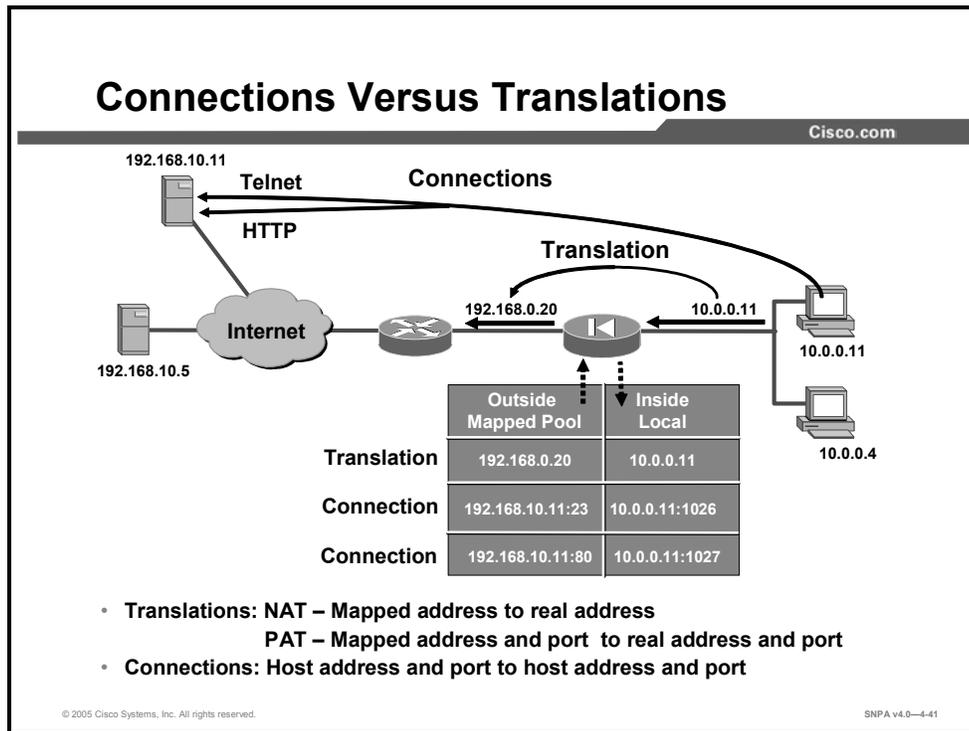
Translations are at the IP layer. For NAT translations, it is the mapped to real IP address. For PAT translations, it is the mapped address and mapped port number to the real address and real port number. Connections are at the transport layer—specifically, TCP. Connections are from a host and port number to a host and port number. Connections are subsets of translations. You can have many connections open that are all utilizing one address translation.

show conn **Command**

Cisco.com

Connection

Internet

192.168.10.11

10.0.0.11

10.0.0.4

pixfirewall#

```
show conn
```

• **Enables you to view all active connections**

```
fw1#show conn
2 in use, 2 most used
fw1# show conn
2 in use, 9 most used
TCP out 192.168.10.11:80 in 10.0.0.11:2824 idle 0:00:03 bytes 2320 flags UIO
TCP out 192.168.10.11:80 in 10.0.0.11:2823 idle 0:00:03 bytes 3236 flags UIO
```

SNPA v4.0—4-42

The **show conn** command displays the number of active TCP connections and information about them. In the figure, there are two connections between host 10.0.0.11 and web server 192.168.10.11. Connections are addressed to TCP port 80 on the web server. The replies are addressed to host 10.0.0.11, ports 2824 and 2823.

The syntax for the **show conn** command is as follows:

```
show conn [count] | [detail]|[protocol tcp | udp |
protocol][{foreign | local} ip [-ip2] [netmask mask]] [{lport
| fport} port1 [-port2]]
```

show conn Command

count	Displays only the number of used connections. The precision of the displayed count may vary depending on traffic volume and the type of traffic passing through the security appliance.
detail	If specified, displays translation type and interface information.
protocol tcp	udp	*protocol*	Displays active connections by protocol type. *protocol* is a protocol specified by number.
{foreign	local} *ip* [*-ip2]* netmask *mask*	Displays active connections by the foreign IP address or the local IP address. Qualifies foreign or local active connections by network mask.
{lport	fport} *port1* [*-port2]*	Displays foreign or local active connections by port.

show conn detail Command

Cisco.com
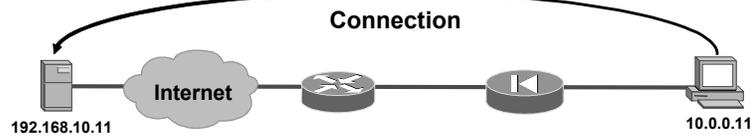
Connection

Internet

192.168.10.11   10.0.0.11

```
fw1# show conn
2 in use, 9 most used
TCP out 192.168.10.11:80 in 10.0.0.11:2824 idle 0:00:03 bytes 2320 flags UIO
TCP out 192.168.10.11:80 in 10.0.0.11:2823 idle 0:00:03 bytes 3236 flags UIO
fw1# show conn detail
2 in use, 9 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, C - CTIQBE media, D - DNS, d - dump,
       E - outside back connection, F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, k - Skinny media,
       M - SMTP data, m - SIP media, O - outbound data, P - inside back conn,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP RPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up
TCP outside:192.168.10.11/80 inside:10.0.0.11/2824 flags UIO
TCP outside:192.168.10.11/80 inside:10.0.0.11/2823 flags UIO
```

SNPA v4.0—4-43

When you use the **show conn detail** option, the system displays information about the translation type, interface information, the IP address and port number, and connection flags. In the figure, the two connections display a flag value of **UIO**. This means that the connections are up with inbound and outbound data.

show local-host Command

Connection

Internet

192.168.10.11   10.0.0.11
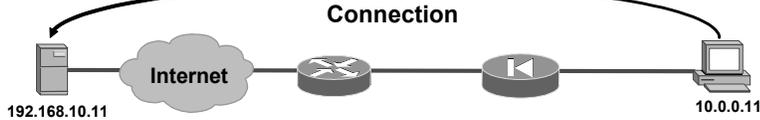
```
fw1# show local-host
Interface dmz: 0 active, 0 maximum active, 0 denied
Interface inside: 1 active, 5 maximum active, 0 denied
local host: < 10.0.0.11 >,
    TCP flow count/limit = 2/300
    TCP embryonic count to host = 0
    TCP intercept watermark = 25
    UDP flow count/limit = 0/unlimited

  Conn:
    TCP out 192.168.10.11 :80 in 10.0.0.11 :2824 idle 0:00:05 bytes 466 flags UIO
    TCP out 192.168.10.11 :80 in 10.0.0.11 :2823 idle 0:00:05 bytes 1402 flags UIO

Interface outside: 1 active, 1 maximum active, 0 denied
local host: < 192.168.10.11 >,
    TCP flow count/limit = 2/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited

  Conn:
    TCP out 192.168.10.11 :80 in insidehost:2824 idle 0:00:05 bytes 466 flags UIO
    TCP out 192.168.10.11 :80 in insidehost:2823 idle 0:00:05 bytes 1402 flags UIO
```

SNPA v4.0—4-44

The **show local-host** command enables you to display the network states of local hosts. A local host is created for any host that forwards traffic to or through the security appliance. This command lets you show the translation and connection slots for the local hosts. In the figure, the inside host 10.0.0.11 establishes two web connections with server 192.168.10.11. The output of **show local-host** is displayed.

This command also displays the connection limit values. In the figure, the current TCP flow count for local host 10.0.0.11is 2 with a limit of 300. If a connection limit is not set, the value displays as "unlimited." In the event of a SYN attack (with TCP Intercept configured), the **show local-host** command output includes the TCP embryonic count to host and the TCP Intercept watermark. In the figure, the embryonic threshold is set for local host 10.0.0.11 at 25 and the current number of embryonic connections is 0.

You can use the command **clear local-host** [*ip_address*], to clear the network state of all local hosts or of a specific IP address. It stops all connections and translations that are associated with the local hosts or with the specific IP address specified in the command.

The syntax for the **local-host** command is as follows:

```
clear local-host [ip_address]
show local-host [ip_address]
```

local-host Command

ip_address	(Optional) Local host IP address.

show xlate Command

Cisco.com

Translation

192.168.0.20   10.0.0.11

Internet

192.168.10.11

10.0.0.11

10.0.0.4
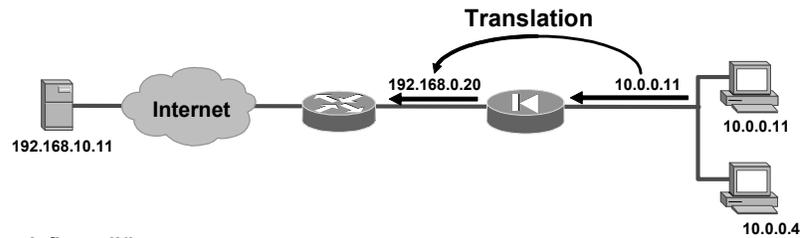
pixfirewall#

```
show xlate
```

• **Enables you to view translation slot information**

```
fw1#show xlate
1 in use, 2 most used
Global 192.168.0.20 Local 10.0.0.11
```

SNPA v4.0—4-45

The **xlate** command enables you to show or clear the contents of the translation slots. Always use **clear xlate** or **reload** after adding, changing, or removing **access-list**, **global**, **nat**, **route**, or **static** commands in your configuration. In the figure, host 10.0.0.11 is translated to a global address of 192.168.0.20 by the security appliance.

The syntax for the **xlate** command is as follows:

```
clear xlate [mapped_ip [local_ip]]
show xlate [mapped_ip [local_ip]]
```

xlate Command

mapped_ip	The registered IP address to be used from the mapped pool.
local_ip	The local IP address from the inside network.

The **show timeout** command displays the idle time limit for connection and translation slots. If the slot has not been used for the idle time specified, the resource is returned to the free pool. TCP connection slots are freed approximately 60 seconds after a normal connection close sequence.

The following is sample output from the **show timeout** command:

```
show timeout
```

```
timeout xlate 3:00:00
```

```
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
```

show xlate detail Command

Translation

Internet

192.168.0.20   10.0.0.11

192.168.10.11   10.0.0.11
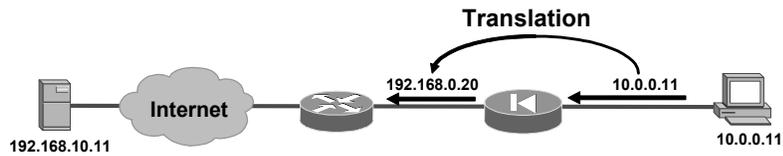
```
fw1#show xlate
1 in use, 3 most used
Global 192.168.0.20 Local 10.0.0.11
fw1# show xlate detail
1 in use, 3 most used
Flags: D - DNS, d - dump, I - identity, i - dynamic, n - no random, r - portmap, s
   - static
NAT from inside:10.0.0.11 to outside:192.168.0.20 flags i
```

SNPA v4.0—4-46

When you use the **show xlate detail** option, the system displays information about the
translation, interface information, the IP address, and the type of translation. In the figure, the
translation displays a flag value of **i**. This means that the translation is a dynamic translation.

Security Appliance NAT Philosophy

Outside   **Inside**

Internet

192.168.10.11   192.168.0.20   10.0.0.11   10.0.0.11

NAT   10.0.0.4
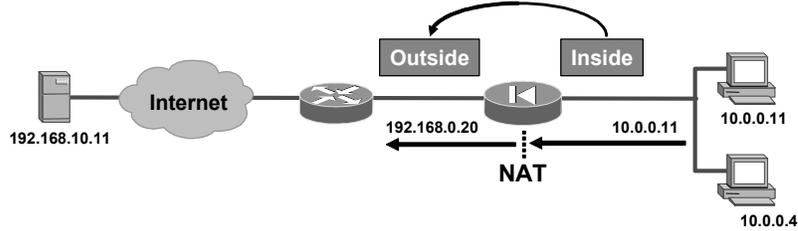
- **Security appliance translation rules are configured between pairs of interfaces.**
- **With NAT control enabled, a packet cannot be switched across the security appliance if it does not match a translation slot in the translation table except for NAT 0, which doesn't create a translation entry.**
- **If there is no translation slot, the security appliance will try to create a translation slot from its translation rules.**
- **If no translation slot match is found, the packet is dropped.**

SNPA v4.0—4-47

With NAT control enabled, translations are built for every source-destination interface pair. This permits the security appliance to translate the real internal host to mapped addresses depending on the destination. A packet will not be forwarded by the security appliance if the packet does not match any of the existing translation entries or if a translation entry cannot be established according to the translation rules. NAT 0 is a translation rule that does not translate an address and does not use a translation slot.

Matching Outbound Packet Addresses

- **A packet arrives at an inside interface:**
  - **The security appliance consults the access rules first.**
  - **The security appliance makes a routing decision to determine the outbound interface.**
- **The source address is checked against the local addresses in the translation table:**
  - **If found, the source address is translated according to the translation slot.**
- **Otherwise the security appliance looks for a match to the local address in the following order:**
  - nat0 access-list **(NAT exemption) – In order, until first match**
  - static **(static NAT) – In order, until first match**
  - static {tcp | udp} **(static PAT) – In order, until first match**
  - nat *nat_id* access-list **(policy NAT) – In order, until first match**
  - nat **(regular NAT): Best match**
- **If no match is found, the packet is dropped.**

For outbound connections with NAT control enabled, the destination interface is evaluated according to the routing table; it must be at a lower security level than the originating interface unless same-security-traffic is permitted. The security appliance then compares the source address with the inside-local entries in the translation table. If a match is found, the translation is used. If no translation for this source-destination interface pair exists, the security appliance matches local traffic to translation commands in the following order:

- **nat 0 access-list** (NAT exemption)—In order, until the first match. For example, you could have overlapping local and destination addresses in multiple **nat** commands, but only the first command is matched.

- **static** (static NAT)—In order, until the first match. Because you cannot use the same local address in static NAT or static PAT commands, the order of **static** commands does not matter. Similarly, for static policy NAT, you cannot use the same local and destination addresses and port across multiple statements.

- **static** {**tcp** | **udp**} (static PAT)—In order, until the first match. Because you cannot use the same local address in static NAT or static PAT commands, the order of **static** commands does not matter. Similarly, for static policy NAT, you cannot use the same local/destination address and port across multiple statements.

- **nat** *nat_id* **access-list** (policy NAT)—In order, until the first match. For example, you could have overlapping local and destination ports and addresses in multiple **nat** commands, but only the first command is matched.

- **nat** (regular NAT)—Best match. The order of the **nat** commands does not matter. The **nat** command that best matches the local traffic is used. For example, you can create a general statement to translate all addresses (0.0.0.0) on an interface. If you also create a statement to translate only 10.1.1.1, then when 10.1.1.1 makes a connection, the specific statement for 10.1.1.1 is used because it matches the local traffic best.

- If you configure multiple **global** commands on the same NAT ID, they are used in this order:

    — None if using NAT 0(identity NAT)

    — Dynamic NAT

    — PAT

A new translation is created according to the translation rules. With NAT control enabled, the security appliance enforces address translation. When no matching translation rule for this new connection is found, the packet is dropped. With NAT control disabled when no match for this new connection is found, the NAT is not applied to the packet and the packet is forwarded if the security policy permits it.

Configuring Multiple Interfaces

This topic describes how to configure multiple interfaces on Cisco security appliances.

Additional Interface Support

e3 Partner Network
Security Level 50

e2 DMZ
Security Level 30

e4 Intranet
Security Level 70

Internet

e0 Outside
Security Level 0

e1 Inside
Security Level 100

- **Supports additional interfaces**
- **Increases the security of publicly available services**
- **Easily interconnects multiple extranets and partner networks**
- **Easily configured with standard security appliance commands**

SNPA v4.0—4-50

Cisco security appliances support up to 12 additional physical interfaces for platform extensibility and security policy enforcement on publicly accessible services. The multiple physical interfaces enable Cisco security appliances to protect publicly accessible web, mail, and DNS servers on the DMZ. Web-based and traditional electronic data interchange (EDI) applications that link vendors and customers are also more secure and scalable when implemented using a physically separate network. Even as the trend toward building these intranet and partner network applications is accelerating, Cisco security appliances are already prepared to accommodate them.

Configuring Three Interfaces

Cisco.com

```
fw1(config)# interface ethernet0
fw1(config-if)# nameif outside
fw1(config-if)# ip address 192.168.0.2
  255.255.255.0
fw1(config)# interface ethernet1
fw1(config-if)# nameif inside
fw1(config-if)# ip address 10.0.0.1 255.255.255.0
  fw1(config)# interface ethernet2
fw1(config-if)# nameif dmz
fw1(config-if)# sec 50
fw1(config-if)# ip address 172.16.0.1 255.255.255.0

fw1(config)# nat (inside) 1 10.0.0.0 255.255.255.0
fw1(config)# global (outside) 1 192.168.0.20-
  192.168.0.254 netmask 255.255.255.0

fw1(config)# static (dmz,outside) 192.168.0.11
  172.16.0.2 netmask 255.255.255.255

fw1(config)# static (inside,dmz) 10.0.0.0 10.0.0.0
  netmask 255.255.255.0
```
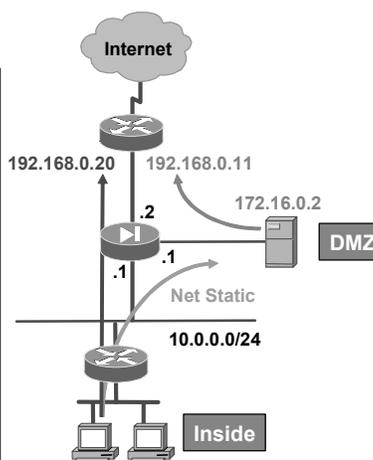
SNPA v4.0—4-51

A third interface is configured as shown in the figure. When your security appliance is equipped with three or more interfaces, use the following guidelines to configure it while employing NAT:

- An interface is always outside with respect to another interface that has a higher security level. By default, packets cannot flow between interfaces that have the same security level unless the **same-security-traffic** command is enabled.

- Use the **nat** command to let users on the respective interfaces start outbound connections. Associate the NAT ID in the **nat** command with the NAT ID in the **global** command.

- The **net static** implementation permanently maps host addresses on one subnet to another subnet on a lower security interface. It is recommended when you want to translate multiple hosts on one subnet to another using a single command.

- After you have completed a configuration in which you add, change, or remove a **global** statement, save the configuration and enter the **clear xlate** command so that the IP addresses will be updated in the translation table.

- To permit access to servers on protected networks from a less secure interface, use the **static** and **access-list** commands.

In the figure, hosts on the inside network can access the outside network. The real 10.0.0.0/24 address is assigned a mapped address from the mapped pool 192.168.0.20–254. When an inside host accesses the DMZ, the real address is statically mapped to itself using a single command. Last, the DMZ server is always translated to an outside address of 192.168.0.11.

Configuring Four Interfaces

```
fw1(config)# interface ethernet0
fw1(config-if)# nameif outside
fw1(config-if)# ip address 192.168.0.2
  255.255.255.0
fw1(config)# interface ethernet1
fw1(config-if)# nameif inside
fw1(config-if)# ip address 10.0.0.1 255.255.255.0
fw1(config)# interface ethernet2
fw1(config-if)# nameif dmz
fw1(config-if)# sec 50
fw1(config-if)# ip address 172.16.0.1 255.255.255.0
fw1(config)# interface ethernet3
fw1(config-if)# nameif partnernet
fw1(config-if)# sec 40
fw1(config-if)# ip address 172.18.0.1 255.255.255.0

fw1(config)# nat (inside) 1 10.0.0.0 255.255.255.0
fw1(config)# global (outside) 1 192.168.0.20-
  192.168.0.254 netmask 255.255.255.0

fw1(config)# static (inside,dmz) 10.0.0.0 10.0.0.0
  netmask 255.255.255.0

fw1(config)# static (dmz,outside) 192.168.0.11
  172.16.0.2
fw1(config)# static (dmz,partnernet) 172.18.0.11
  172.16.0.2
```
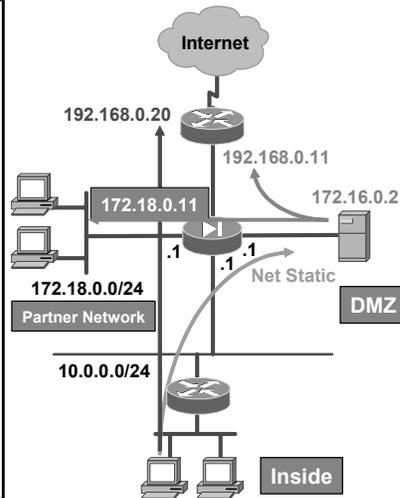

SNPA v4.0—4-52

In the figure, the security appliance has four interfaces. Users on the inside have access to the DMZ and the outside. The server 172.16.0.2 is visible on the outside as 192.168.0.11 and on the partner network as 172.18.0.11. Configuring four interfaces requires more attention to detail, but they are configured with standard security appliance commands. To enable users on a higher security level interface to access hosts on a lower security interface, use the **nat** and **global** commands (for example, when users on the inside interface have access to the Internet).

To let users on a lower security level interface, such as users on the partner network interface, access hosts on a higher security interface (DMZ), use the **static** and **access-list** commands. As seen in the figure, the partner network has a security level of 40 and the DMZ has a security level of 50. The DMZ will use **nat** and **global** commands to speak with the partner network and will use **static** commands and **access-list** commands to receive traffic originating from the partner network.

Summary

This topic summarizes what you learned in this lesson.

Summary

- **The security appliance manages the TCP and UDP protocols through the use of a translation table (for NAT sessions) and a connection table (for TCP and UDP sessions).**
- **The** static **command creates a permanent translation.**
- **Mapping between local and global address pools is done dynamically with the** nat **command.**
- **The** nat **and** global **commands work together to hide internal IP addresses.**
- **The security appliance supports PAT.**
- **Configuring multiple interfaces requires a greater attention to detail, but can be done with standard security appliance commands.**

SNPA v4.0—4-53

Access Control Lists and Content Filtering

Overview

This lesson discusses how to control access through Cisco security appliances using access control lists (ACLs). A general discussion of ACLs is provided along with detailed examples of special-use ACLs. The lesson then shows you how to configure Cisco security appliances to filter malicious active codes and concludes with a discussion on how to configure URL filtering.

Objectives

Upon completing this lesson, you will be able configure security appliance access control. This includes being able to meet these objectives:

- Configure and explain the basic function of ACLs
- Configure and explain additional functions of ACLs
- Configure active code filtering (ActiveX and Java applets)
- Configure the security appliance for URL filtering

ACLs

This topic discusses access control through Cisco security appliances using ACLs.

Security Levels Revisited

Outbound

Less secure ← **More secure**

Internet

Outside
security level **0**

Inside
security level **100**

Less secure → **More secure**
Inbound

- **Security levels tag the security appliance interface with a number, 0 being the least secure and 100 being the most secure.**
- **Security levels enable the security appliance to identify whether a requested session is inbound or outbound:**
  - **Inbound session is a session from a less secure to a more secure interface**
  - **Outbound session is a session from a more secure to a less secure interface**

SNPA v4.0—5-4

The configuration of every security appliance defaults to an inside interface with a level of 100 and an outside interface with a level of 0. There is nothing more secure than the internal network and nothing less secure than the external network. After address translation is configured, by default all communications are permitted in an outbound direction, from a more secure level to a less secure level. And by default all communications are prohibited in an inbound direction, from a less secure level to a more secure level.

Security Appliance ACL Configuration

Internet — Outside — Inside

ACL for inbound access → ← **ACL for outbound access**

No ACL
- **Outbound permitted by default**
- **Inbound denied by default**
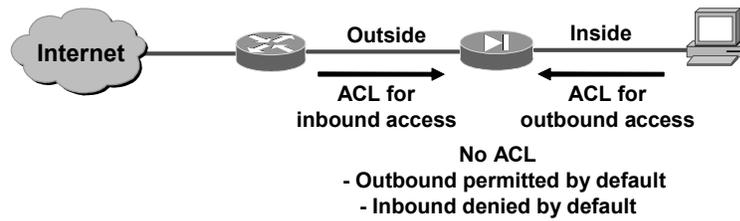
Security appliance configuration philosophy is interface based.
- **Interface ACL permits or denies the initial packet *incoming* or *outgoing* on that interface.**
- **ACL needs to describe only the initial packet of the application; no need to think about return traffic.**
- **If no ACL is attached to an interface, the following ASA policy applies:**
  - **Outbound packet is permitted by default.**
  - **Inbound packet is denied by default.**

SNPA v4.0—5-5

ACLs can work in both directions, but are evaluated only once per connection. After an ACL is configured, it is activated with an **access-group** command. If no ACL is attached to an interface, then outbound traffic is permitted by default unless explicitly denied and inbound traffic is denied by default unless explicitly permitted.

ACL Usage Guidelines

- **Higher to lower security level:**
  - **Use an ACL to restrict outbound traffic.**
  - **The ACL source address is the actual (untranslated) address of the host or network.**
- **Lower to higher security level:**
  - **Use an ACL to enable inbound traffic.**
  - **Use an ACL to restrict inbound protocols.**
  - **The ACL destination address is the translated global IP address.**

SNPA v4.0—5-6

The **access-list** command is used to permit or deny traffic. The following are guidelines for designing and implementing ACLs:

- Higher to lower security:

  — The ACL is used to restrict outbound traffic.

  — The source address argument of the ACL command is the actual address of the host or network.

- Lower to higher:

  — The ACL is used to restrict inbound traffic.

  — The destination address argument of the ACL command is the translated global IP address.

Note	ACLs are *always* checked *before* translation is performed on the security appliance.

Inbound HTTP Traffic to DMZ Web Server
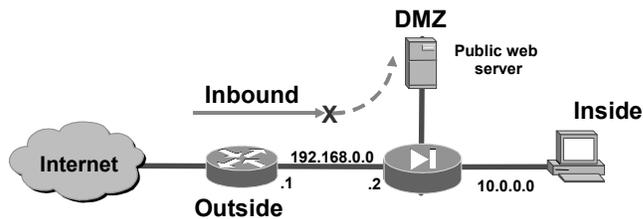
By default, inbound access is denied — no ACL. To permit inbound traffic, complete the following steps:
- Configure static translation for WWW server address.
- Configure inbound access control list.
- Apply access control list to outside interface.

In the figure, a company's network administrator needs to enable Internet users to access the company's public web server. The web server is isolated on the security appliance DMZ. By default, any inbound access to the web server from the Internet is denied. To grant access to Internet users, the administrator must complete the following steps:

- Configure a static translation for the web server address. In this way, the web server address is hidden from the Internet users.

- Configure an inbound ACL that grants access to specific hosts and protocols.

- Apply the ACL to an interface.

Create a Static Translation for Web Server

Cisco.com

DMZ

172.16.0.2 Public web server

192.168.0.9

Inside

192.168.0.0

Internet

.1 Outside .2 10.0.0.0
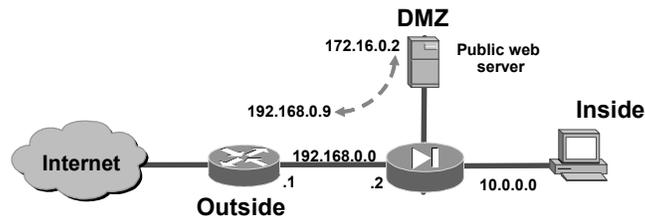
```
fw1(config)# static (dmz,outside) 192.168.0.9
  172.16.0.2 0 0
```

• **Map an inside private address to an outside public address**

SNPA v4.0—5-8

The first step is to map the IP address of the web server to a fixed outside address. This hides the true address of the web server. Internet hosts access the DMZ web server via the mapped outside IP address. The security appliance performs the necessary translations to send the packet from the outside interface to the DMZ interface. To accomplish this, a **static** command is used. The figure shows IP address 192.168.0.9 on the outside interface mapped to 172.16.0.2 on the DMZ.

access-list Command

Cisco.com
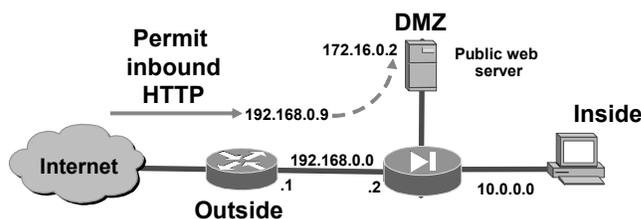

```
firewall(config)#
```

```
access-list id [line line-number] [extended] {deny | permit}
  {tcp | udp} {host sip | sip mask | any}[operator port]
{host dip | dip mask | any}[operator port]
```

• **Permit outside HTTP access to public web server**

```
fw1(config)# access-list aclout permit tcp any host
  192.168.0.9 eq www
```

SNPA v4.0—5-9

The **access-list** command enables you to specify if an IP address is permitted or denied access to a port or protocol. By default, all access to addresses in an ACL is denied. You must explicitly permit it.

When specifying the IP address of a host as a source or destination, use the host keyword instead of the network mask 255.255.255.255. For example, use the following ACL entry to permit Hypertext Transfer Protocol (HTTP) traffic from any host to host 192.168.0.9:

```
access-list aclout permit tcp any host 192.168.0.9 eq www
```

The **show access-list** command lists the **access-list** command statements in the configuration. The **show access-list** command also lists a hit count that indicates the number of times an element has been matched during an **access-list** command search.

The **clear access-list** command removes all references in the security appliance configuration to a deleted ACL. If the *acl_id* argument is specified, it clears only the corresponding ACL. If the **counters** option is specified as well, it clears the hit count for the specified ACL. To clear an ACL from the running configuration, use the **clear configure access-list** command.

The **no access-list** command removes an **access-list** command from the configuration. If you remove all the **access-list** command statements that are in an ACL group, the **no access-list** command also removes the corresponding **access-group** command from the configuration.

Note	The **access-list** command uses the same syntax as the Cisco IOS software **access-list** command except that the subnet mask in the security appliance **access-list** command is reversed from the Cisco IOS software version of this command. For example, a wildcard mask specified as 0.0.0.255 in the Cisco IOS **access-list** command would be specified as a subnet mask of 255.255.255.0 in the security appliance **access-list** command.

The syntax for the **access-list** commands is as follows:

```
access-list id [line line-number] [extended] {deny |
permit}{protocol | object-group protocol_obj_grp_id}{host sip
| sip mask | interface ifc_name | object-group
network_obj_grp_id | any}{host dip | dip mask | interface
ifc_name | object-group network_obj_grp_id | any}[log [[level]
[interval secs] | disable | default]][inactive | time-range
time_range_name]
```

deny	This option does not allow a packet to traverse the security appliance if the conditions are matched. By default, the security appliance denies all inbound and outbound packets unless you specifically permit access.
dip	Specifies the IP address of the network or host to which the packet is being sent. Specify a *dip* when an **access-list** command is used in conjunction with an **access-group** command or in conjunction with an **aaa match access-list** command and **aaa authorization** command. For inbound and outbound connections, *dip* is the address before NAT has been performed.
dip_mask	Netmask bits (mask) to be applied to *dip*.
icmp_type	(Optional) Specifies the ICMP type.
icmp_type_obj_grp_id	(Optional) Specifies the identifier of an existing ICMP-type object group.
id	Specifies the name or number of an ACL.
inactive	Disables an access control element.
interface *ifc_name*	Specifies the interface address as the source or destination address.
interval *secs*	Specifies the log interval at which to generate a syslog message; valid values are from 1 to 600 seconds. Default is 300.
line *line-num*	(Optional) The line number at which to insert an access control element.
**log disable	default |** *level*	(Optional) Specifies that the **log** option is disabled, set to default values, or set to a syslog level from 0 to 7. The default level is 6. When enabled, a syslog message is generated for the access control element. See the **log** command for information.
network_obj_grp_id	Specifies the identifier of an existing network object group.
object-group	Specifies an object group.
operator	Compares sip or dip ports. Possible operands include "lt" (less than), "gt" (greater than), "eq" (equal), "neq" (not equal), and "range" (inclusive range).
permit	The **permit** option selects a packet to traverse the security appliance if conditions are matched. By default, the security appliance denies all inbound and outbound packets unless you specifically permit access.
port	Specifies the decimal number or name of a TCP or User Datagram Protocol (UDP) port.
protocol	Specifies the IP protocol name or number that will be open. For example, UDP is 17, TCP is 6, and exterior gateway protocol (EGP) is 47.
protocol_obj_grp_id	Specifies the identifier of an existing protocol object group.
service_obj_grp_id	Specifies the identifier of an existing service object group.

sip	Specifies the IP address of the network or host from which the packet is being sent.
sip_mask	Netmask bits (mask) to be applied to the source IP address.
time-range *time_range_name*	(Optional) Specifies the time range used to define specific times of the day and week to allow access to the security appliance. See the section on configuring time ranges for information about defining a time range.

Note   For inbound connections, the destination address is the global address. For outbound connections, the source address is the address before NAT has been performed.

access-group Command

Apply access control list to interface

DMZ

Public web server

Inside

Internet

192.168.0.0

.1   .2

10.0.0.0
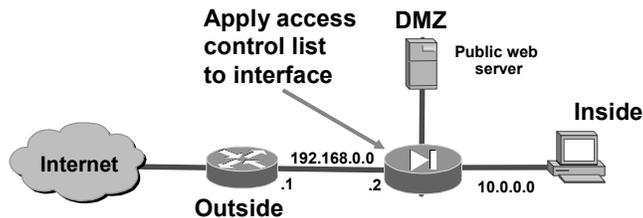
Outside

```
firewall(config)#
access-group access-list {in | out} interface
  interface_name [per-user-override]
```

- **Apply ACL to outside interface**

```
fw1(config)# access-group aclout in interface
  outside
```

The **access-group** command binds an ACL to an interface. The ACL is applied to traffic on an interface in the specified direction, inbound or outbound. Only one ACL can be bound to an interface using the **access-group** command. In the figure, the ACL is bound to the outside interface (**aclout**).

The **no access-group** command unbinds the ACL from the interface.

The **show running-config access-group** command displays access group information.

The **clear configure access-group** command removes all entries from an ACL indexed by the ACL identifier (ID). If the ACL ID is not specified, all **access-group** command statements are removed from the configuration.

The syntax for the **access-group** commands is as follows:

```
access-group access-list {in | out} interface interface_name
[per-user-override]
```

access-list	ACL *id*
in	Filters the inbound packets at the specified interface.
out	Filters the outbound packets at the specified interface.
Interface interface-name	The name of the network interface.
per-user-override	(Optional) Allows downloadable user ACLs to override the ACL applied to the interface.

show access-list Command
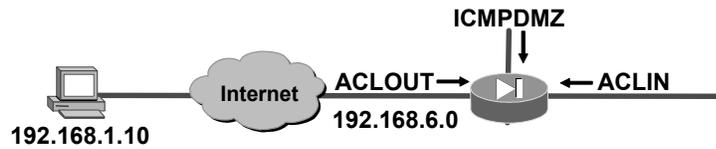
ICMPDMZ

192.168.1.10

Internet

ACLOUT → ← **ACLIN**

192.168.6.0

```
fw1(config)# show access-list
access-list ACLOUT; 4 elements
access-list ACLOUT line 1 permit tcp 192.168.1.0 255.255.255.0 host
  192.168.6.11 eq www (hitcnt=4)
access-list ACLOUT line 2 permit tcp host 192.168.1.10 host 192.168.6.11
  eq ftp (hitcnt=1)
access-list ACLOUT line 3 permit tcp any host 192.168.6.10 eq www
  (hitcnt=4)
access-list ACLOUT line 4 deny ip any any (hitcnt=0)
access-list ICMPDMZ; 1 elements
access-list ICMPDMZ line 1 permit icmp host bastionhost any echo-reply
  (hitcnt=12)
access-list ACLIN; 1 elements
access-list ACLIN line 1 permit tcp any host 192.168.1.10 eq www
  (hitcnt=0)
```

The **show access-list** command lists all the configured ACLs, the counters, and the access control entries (ACEs). In the figure, there are three ACLs: **ACLOUT**, **ICMPDMZ**, and **ACLIN**. Within each ACL, there are one or more ACEs. Each ACE is denoted by a line number. The ACEs are numbered from line 1 to line 6. In the figure, **ACLOUT** has six ACEs.

clear access-list counters Command
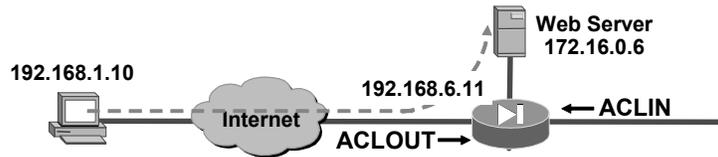

```
fw1(config)# clear access-list aclout counters
fw1(config)# show access-list
access-list ACLOUT; 4 elements
access-list ACLOUT line 1 permit tcp 192.168.1.0 255.255.255.0 host
  192.168.6.11 eq www (hitcnt=0)
access-list ACLOUT line 2 permit tcp host 192.168.1.10 host 192.168.6.11
  eq ftp (hitcnt=0)
access-list ACLOUT line 3 permit tcp any host 192.168.6.10 eq www
  (hitcnt=0)
access-list ACLOUT line 4 deny ip any any (hitcnt=4)
access-list ICMPDMZ; 1 elements
access-list ICMPDMZ line 1 permit icmp host bastionhost any echo-reply
  (hitcnt=10)
access-list ACLIN; 1 elements
access-list ACLIN line 1 permit tcp any host 192.168.1.10 eq www
  (hitcnt=19)
```

The network administrator can use the **clear access-list counters** to troubleshoot network access. In the example, the remote user at 192.168.1.10 is trying to access the server at 172.16.0.6. The outside address for the web server is 192.168.6.11. The administrator can view the show access-list counters to determine whether the source packet reached the security appliance access-list. If the access-list ACLOUT line 1 hitcnt increments, the packet reached the security appliance access-list. If the access-list ACLOUT line 4 extended deny IP any any hitcnt incremented, the packet reached the security appliance but was denied access. If neither access-list hitcnt was incremented. The packet never reached the security appliance access-list. To check the progress of the troubleshooting, the administrator can clear the ACL counters, or hitcnt. The **clear access-list counters** command clears the counters for the specified ACL. If no ACL is specified all the access lists counters are cleared.

Time Range Configuration

DMZ

Web
Server
172.16.0.6

Enable access:
8 AM to 5 PM
1 Aug to 30 Aug

Temp
Worker

Inside

Internet

192.168.0.0

10.0.0.0

.1   .2

.9

192.168.10.2
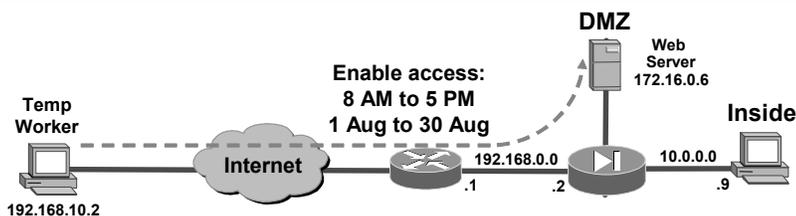
firewall(config)#

```
time-range name
```

- **Define a time when certain resources can be accessed**
- **Apply time-range to ACL**

```
fw1(config)# time-range temp-worker
fw1(config-time-range)#
```

SNPA v4.0—5-13

It is possible to create a time range that defines a time when certain resources can be accessed. After the time range is defined, it can be applied to an ACL. The time range relies on the system clock of the security appliance; however, the feature works best with Network Time Protocol (NTP) synchronization. For example, a company hires temporary worker. The worker needs access to a specific server from 8 a.m. to 5 p.m. for one month. The **time-range** command defines the range of calendar days and access hours.

Time-Range Sub-Mode

Cisco.com

DMZ

Web Server
172.16.0.6

Enable access:
8 AM to 5 PM
1 Aug to 30 Aug

Temp Worker

Inside

Internet

192.168.0.0
.1   .2

10.0.0.0
.9

192.168.10.2
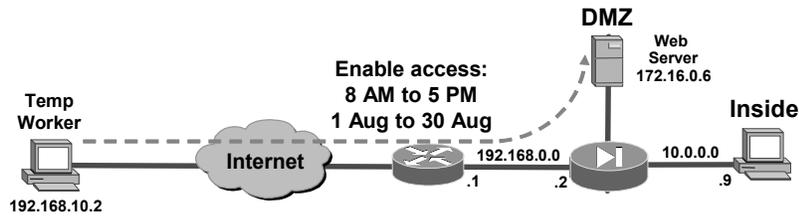
firewall(config)#

```
time-range <name>
  absolute [start <hh:mm> <date>] [end <hh:mm> <date>]
  periodic <days-of-week><hh:mm> to <days-of-week><hh:mm>
```

• **Define a time when certain resources can be accessed**
  • **Absolute start and stop time and date**
  • **Recurring time range time and day of the week**

```
fw1(config)# time-range temp-worker
fw1(config-time-range)# absolute start 00:00 1 August 2005 end
  00:00 30 August 2005
fw1(config-time-range)# periodic weekdays 8:00 to 17:00
```

SNPA v4.0—5-14

The time range submode allows you to configure the various properties of the time range you wish to implement. The following commands are available:

■ **absolute**: Defines an absolute time that a time range is in effect

■ **periodic**: Specifies a recurring (weekly) time range for functions that support the time-range feature

The syntax for the **absolute** command is as follows:

```
absolute [end time date] [start time date]
```

date	Specifies the date in the format of day month year, for example, 1 January 2006. The valid range of years is 1993 through 2035.
time	Specifies the time in the format of HH:MM. For example, 8:00 is 8:00 a.m. and 20:00 is 8:00 p.m.

The syntax for the **periodic** command is as follows:

```
periodic days-of-the-week time to [days-of-the-week] time
```

days-of-the-week	(Optional) The first occurrence of this argument is the starting day or day of the week that the associated time range is in effect. The second occurrence is the ending day or day of the week that the associated statement is in effect.
	This range of days can be any single day or combination of days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. Other possible values are:
	• Daily—Monday through Sunday
	• Weekdays—Monday through Friday
	• Weekend—Saturday and Sunday
	If the ending days of the week are the same as the starting days of the week, you can omit them.
time	Specifies the time in the format HH:MM. For example, 8:00 is 8:00 a.m. and 20:00 is 8:00 p.m.
to	Entry of the **to** keyword is required to complete the range of days.

Time-based Access-list
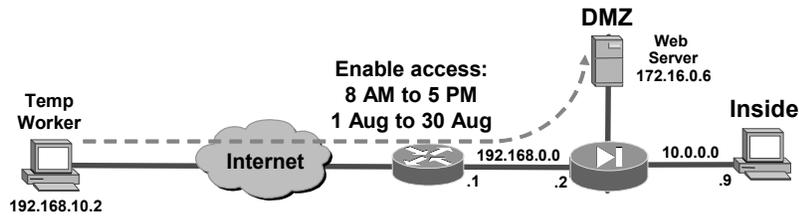
DMZ

Web Server 172.16.0.6

Enable access: 8 AM to 5 PM 1 Aug to 30 Aug

Temp Worker

Inside

Internet

192.168.0.0

10.0.0.0

.1

.2

.9

192.168.10.2

firewall(config)#

```
access-list acl_id [line line-num] {deny | permit}
  protocol source_addr source_mask [operator port[port]]
  destination_addr destination_mask operator port [port]
  [log [[disable | default] | [level]]] [interval secs]
  [time-range [name]]
```

• **Apply time-range to an ACL**

```
fw1(config)# static (dmz,outside) 192.168.0.6 172.16.0.6
fw1(config)# access-list aclin permit tcp host 192.168.10.2
  host 192.168.0.6 eq www time-range temp-worker
```

SNPA v4.0—5-15

In the example in the figure, a time-based ACL is being used. The time range has previously been defined using the **time-range** command and the time range submode. and the time range is named *temp-worker*.

Time-based Access-list Example
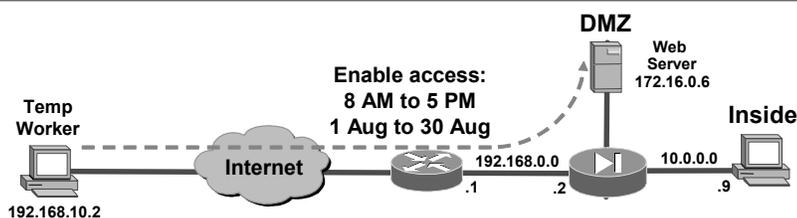
DMZ
Web Server
172.16.0.6

Enable access:
8 AM to 5 PM
1 Aug to 30 Aug

Temp Worker

Inside

Internet

192.168.0.0
.1   .2

10.0.0.0
.9

192.168.10.2

```
fw1(config)# static (dmz,outside) 192.168.0.6 172.16.0.6

fw1(config)# access-list aclin permit tcp host 192.168.10.2 host
  192.168.0.6 eq www time-range temp-worker
fw1# show run time-range
  time-range temp-worker
    absolute start 00:00 1 August 2005 end 17:00 30 August 2005
    periodic weekdays 8:00 to 17:00
fw1(config)# show clock
  13:48:33.226 UTC Sat Jul 30 2005
fw1(config)# show access-list
  access-list aclin; 1 elements
  access-list aclin line 1 extended permit tcp host 192.168.10.2 host
  192.168.0.6 eq 80 time-range temp-worker (hitcnt=0) (inactive)
```

SNPA v4.0—5-16

The example in this figure summarizes various elements of a time-based ACL. In this example, the time range for ACL activation has not been reached, therefore the ACL is marked as inactive.

ACL Logging
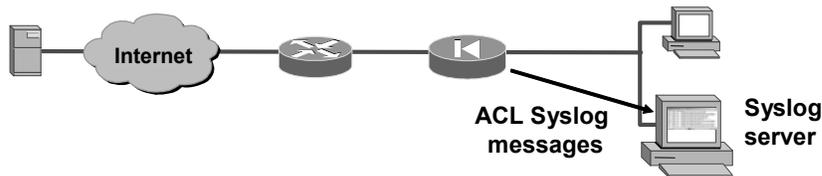
```
firewall(config)#

access-list acl_ID line line-num {deny | permit}
  protocol source_addr source_mask [operator
  port[port]] destination_addr destination_mask
  operator port [port] [log [[disable |default] |
  [level]]] [interval secs]]
```

• **Log option enabled for inbound ICMP to 192.168.1.1**

```
fw1(config)# access-list outside-acl permit icmp any
  host 192.168.1.1 log 7 interval 600
```

The **log** option specifies that syslog message 106100 is generated for the ACE to which it is applied. (Syslog message 106100 is generated for every matching permit or deny ACE flow that passes through the security appliance.) The first-match flow is cached. Subsequent matches increment the hit count displayed in the **show access-list** command for the ACE. New 106100 messages will be generated at the end of the interval defined by **interval** *secs* if the hit count for the flow is not 0.

The following example illustrates the use of ACL-based logging in an ICMP context:

1. An inbound ICMP echo request to 192.168.1.1 arrives on the outside interface.

2. An ACL called **outside-acl** is applied for the access check.

3. The packet is permitted by the first ACE of **outside-acl**, which has the **log** option enabled.

4. The log flow (ICMP, 192.168.10.12, 0, 192.168.1.1, 8) has not been cached, so the following syslog message is generated and the log flow is cached:

    ```
    106100: access-list outside-acl permitted icmp
    outside/192.168.10.12(0) -> inside/192.168.1.1(8) hit-cnt 1
    (first hit)
    ```

5. Within the next 10 minutes (600 seconds), 20 such packets arrive on the outside interface. Because the log flow has been cached, the log flow is located and the hit count of the log flow is incremented for each packet.

6. At the end of the 10th minute, the following syslog message is generated and the hit count of the log flow is reset to 0:

    ```
    106100: access-list outside-acl permitted icmp
    outside/192.168.10.12(0) -> inside/192.168.1.1(8) hit-cnt 20
    (600-second interval)
    ```

7. No such packets arrive on the outside interface within the next 10 minutes. The hit count of the log flow remains 0.

8. At the end of the 20th minute, the cached flow (ICMP, 192.168.10.12, 0, 192.168.1.1, 8) is deleted because of the 0 hit count.

access-list deny-flow-max/ alert-interval

Cisco.com

Internet

DOS attack

**Msg 106101
Deny-Flow reached**

**Syslog
server**
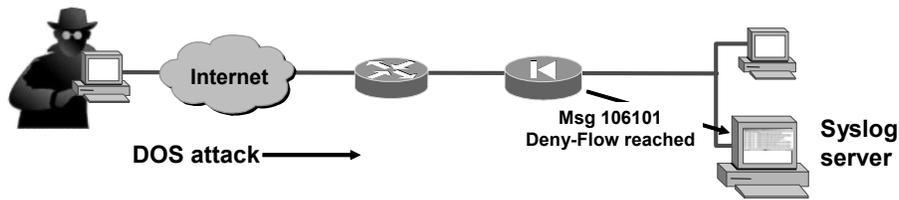
firewall(config)#

```
access-list deny-flow-max <n>
access-list alert-interval <secs>
```

• **Specify the maximum number of concurrent deny-flows**
• **Specify the time interval at which to generate deny-flow
  reached msg (msg 106101).**

```
fw1(config)# access-list deny-flow-max 1024

fw1(config)# access-list alert-interval 120
```

SNPA v4.0—5-18

The **deny-flow-max** parameter is used to specify the maximum number of concurrent deny flows that can be created. The default is 4096. The **alert-level** parameter is used to specify the time interval between deny flow maximum messages. The default is 300 seconds.

ACL Line Number

```
fw1(config)# show access-list
access-list aclout line 2 permit tcp any host
   192.168.0.7 eq www (hitcnt=0)
access-list aclout line 3 permit tcp any host
   192.168.0.8 eq www (hitcnt=0)              ⟸ Insert
access-list aclout line 4 permit tcp any host
   192.168.0.10 eq www (hitcnt=0)
access-list aclout line 5 permit tcp any host
   192.168.0.11 eq www (hitcnt=0)
```

```
access-list id [line line-number] [extended] {deny |
  permit} {tcp | udp} {host sip | sip mask | any}
  [operator port]{host dip | dip mask | any}[operator
  port]
```

- **Insert ACE into existing ACL**

```
fw1(config)# access-list aclout line 4 permit tcp any
  host 192.168.0.9 eq www
```

To view the configured ACLs, use the **show access-list** command. Notice that the **access-list** commands are listed by ACL line number. The line number was not part of the original command line; it was added by the operating system. Individual ACEs are given a single line number. All ACEs pertaining to an object group are given the same line number.

Line numbers give the administrator the ability to insert or delete ACEs within a list of existing ACEs. Use the **access-list** *id* **line** *line-number* command to insert an **access-list** command statement, and use the **no access-list** *id* **line** *line-number* command to delete an **access-list** command statement. Each ACE and remark has an associated line number. Line numbers can be used to insert or delete elements at any position in an ACL. These numbers are maintained internally in increasing order, starting from 1 (for example, in a sequence such as 1, 2, 3 …). A user can insert a new entry between two consecutive ACEs by choosing the line number of the ACE with the higher line number. The line numbers are always maintained in increasing order, with an individual line number for each ACE. However, all ACEs resulting from a single object group **access-list** command statement have a single line number. Consequently, you cannot insert an ACE in the middle of object group ACEs. Line numbers are displayed by the **show access-list** command. However, they are not shown in your configuration.

In the figure, the administrator adds an ACE to the existing ACL. Entering "line 4" in the **access-list** command line inserts this command into the fourth position in the ACL. This forces the existing line 4 ACE to move down one position in the ACL, so it becomes the fifth ACE, and so on.

ACL Comments

```
fw1(config)# show access-list
access-list aclout line 1 remark web server 1 http
    access-list
access-list aclout line 2 permit tcp any host
    192.168.0.8 eq www (hitcnt=0)
access-list aclout line 3 remark web server 2 http
    access-list
access-list aclout line 4 permit tcp any host
    192.168.0.11 eq www (hitcnt=0)
```

firewall(config)#

```
 access-list id [line line-num] remark text
```

• **ACL remark**

```
fw1(config)# access-list outside line 1 remark web
  server http access-list
```

The **access-list remark** command enables users to include comments (remarks) about entries in any ACL. You can use remarks to make the ACL easier to scan and interpret. Each remark line is limited to 100 characters. The ACL remark can be placed before or after an **access-list** command statement, but it should be placed in a consistent position so that it is clear which remark describes which **access-list** command. For example, it would be confusing to have some remarks before the associated **access-list** commands and some remarks after the associated **access-list** commands. In the figure, the administrator added remarks pertaining to the line 3 and line 5 ACEs. The new remarks are the line 2 and line 4 ACEs. To add a remark above an existing ACL entry, type in the ACL remark using the existing ACE line number. The remark forces the existing ACE down. To view existing ACL entries, use the **show access-list** command.

The syntax for the **access-list remark** commands is as follows:

```
access-list remark
access-list id [line line-num] remark text
```

id	Name of an ACL. You can use either a name or number.
line *line-num*	The line number at which to insert a remark or an ACE.
remark *text*	The text of the remark to add before or after an **access-list** command statement, up to 100 characters in length.

Inbound HTTP Access Solution

DMZ

172.16.0.2 — Public WWW Server

Inbound

192.168.0.9

Inside

Internet

192.168.0.0

Outside

.1 .2

10.0.0.0
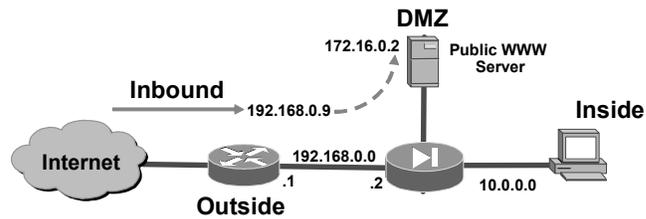
```
fw1(config)# static (DMZ,outside) 192.168.0.9
  172.16.0.2 0 0

fw1(config)# access-list aclout permit tcp any host
  192.168.0.9 eq www

fw1(config)# access-group aclout in interface outside
```

• **Permit outside HTTP access to public web server**

SNPA v4.0—5-21

The figure shows a solution to permit HTTP access to the public web server on the DMZ from the Internet. The **static** command was configured to translate the web server IP address to an outside IP address. An ACL was configured to enable Internet hosts to connect to the web server with HTTP traffic.

Inbound HTTPS Access Solution

DMZ

172.30.4.2 E-Banking web server

Inbound

192.168.0.10

Internet

192.168.0.0

.1 .2

Outside

10.0.0.0

Inside
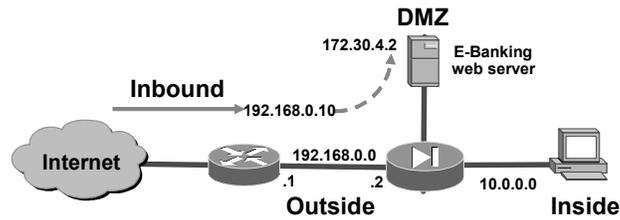
```
fw1(config)# static (DMZ,outside) 192.168.0.10
  172.30.4.2 0 0
fw1(config)# access-list aclout permit tcp any host
  192.168.0.10 eq https
fw1(config)# access-group aclout in interface outside
```

• **Permit outside HTTPs access to e-banking web server**

SNPA v4.0—5-22

In the example in the figure, a company locates its e-banking solution on the DMZ. The administrator wants to establish secure communications between the Internet users and the e-banking web server. To establish an inbound HTTP secure (HTTPS) connection, the administrator configured a static, an ACL, and applied the ACL to an interface.

icmp Command

Cisco.com
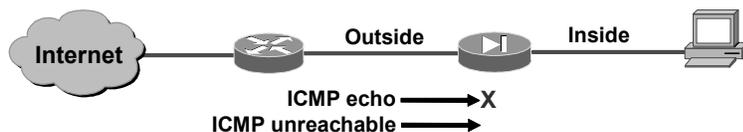
```
firewall(config)#
```

```
icmp {permit | deny} src_addr src_mask [icmp-type]
  if_name
```

- Enables or disables pinging to an interface
- All ping requests denied at the outside interface, and all unreachable messages permitted at the outside interface

```
fw1(config)# icmp permit any echo-reply outside
```

```
fw1(config)# icmp permit any unreachable outside
```

SNPA v4.0—5-23

You can enable or disable pinging to the security appliance interface. With pinging disabled, the security appliance cannot be detected on the network. The **icmp** command implements this feature, which is also referred to as configurable proxy pinging.

Note	By default, pinging through the security appliance to a security appliance interface is not allowed. Pinging an interface from a host on that interface is allowed.

To use the **icmp** command, configure an **icmp** command statement that permits or denies ICMP traffic that terminates at the security appliance. If the first matched entry is a permit entry, the ICMP packet continues to be processed. If the first matched entry is a deny entry or an entry is not matched, the security appliance discards the ICMP packet and generates a 313001 syslog message. An exception is when an **icmp** command statement is not configured, in which case, permission is assumed.

Note	Cisco recommends that you grant permission for the ICMP unreachable message type (type 3). Denying ICMP unreachable messages disables ICMP Path Maximum Transmission Unit (MTU) Discovery, which can halt both IPSec and Point-to-Point Tunneling Protocol (PPTP) traffic. See RFC 1195 and RFC 1435 for details about Path MTU Discovery.

The **clear icmp** command removes **icmp** command statements from the configuration.

The syntax for the **icmp** commands is as follows:

```
icmp {permit | deny} ip_address net_mask [icmp-type] if_name
clear icmp
show icmp
```

deny	Deny access if the conditions are matched.
icmp-type	(Optional) ICMP message type as described in the "ICMP Type Literals" table.
if_name	The interface name.
ip_address	The IP address of the host that is sending ICMP messages to the interface.
net_mask	The mask that is to be applied to *ip_address*.
permit	Permit access if the conditions are matched.

The following table lists the ICMP Type Literals that can be used in the *icmp-type* argument of the **icmp** command to designate which message types are permitted or denied:

ICMP Type Literals

ICMP	Type Literal
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-reply
14	timestamp-request
15	information-request
16	information-reply
17	mask-request
18	mask-reply
31	conversion-error
32	mobile-redirect

Other ACL Uses—
nat0 plus acl command

Cisco.com

Command plus an ACL
• **Identify traffic flow via an ACL**
• **Apply command to the identified traffic flow**

Corporate office

VPN (NAT 0)

Internet

10.100.1.0 /24

**Small office/
home office**

Web
(NAT)
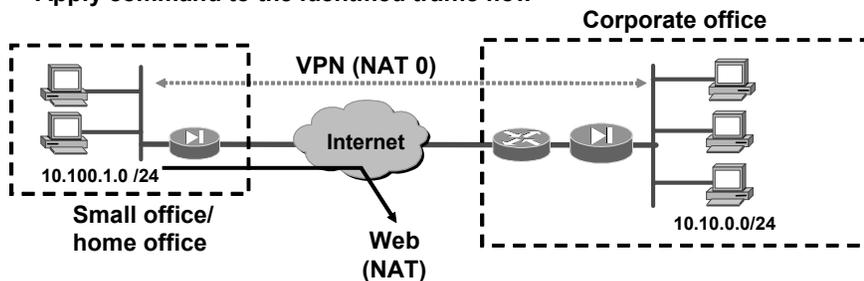
10.10.0.0/24

• **Identify Site-to-site traffic (ACL) not to be translated.**
  • **access-list VPN-NO-NAT** permit ip 10.100.1.0 255.255.255.0 10.10.0.0 255.255.255.0
  • **nat (inside) 0 access-list VPN-NO-NAT**
  • **nat (inside) 1**

SNPA v4.0—5-24

In the previous pages, ACLs were used to identify traffic that was to be either permitted or denied at an interface. ACLs can also be combined with a command. The ACL identifies a flow of traffic. The command associates an action to be performed on the identified traffic. In the example in the figure, there is a small office/home office (SOHO) application. The administrator desires all traffic from the SOHO that is bound for the Internet to be translated And all SOHO traffic that is bound for the corporate office to not be translated. As explained in a previous lesson, the **nat 0** command enables you to exempt a host or network from NAT. The **nat 0 access-list** command takes this a step further by enabling the administrator to exempt from NAT any traffic that is matched by an **access-list** entry. In the example, **VPN_NO_NAT** identifies a traffic flow between 10.100.1.0/24 and 10.10.0.0/24. The VPN_NO_NAT ACL is applied to the **nat 0** command **nat (inside) 0 access-list VPN_NO_NAT**. The **nat 0 access-list** command permits internal hosts on 10.100.1.0/24 subnet to bypass NAT when connecting to corporate hosts on the 10.10.0.0/24 subnet. The **nat 0 access-list** command is usually used in virtual private network (VPN) scenarios.

The syntax of the **nat 0 access-list** command is as follows:

```
nat [(real_ifc)] 0 access-list access_list_name
```

real_if	Name of the network interface, as specified by the **name_if** command, through which the hosts or networks that are designated by a real IP address are accessed.
access-list *access_list_name*	Identifies the local addresses and destination addresses using an extended ACL, also known as policy NAT. Create the ACL using the **access-list** command. This ACL should include only permitted ACEs. You can optionally specify the local and destination ports in the ACL using the **eq** operator. If the NAT ID is 0, then the ACL specifies addresses that are exempt from NAT. NAT exemption is not the same as policy NAT—you cannot specify the port addresses, for example.

Policy NAT— *nat* plus *acl* command

Cisco.com

Company A
192.168.10.11

Company B
192.168.100.4

Internet

ABC Corp.

192.168.0.33

192.168.0.49

10.0.0.15
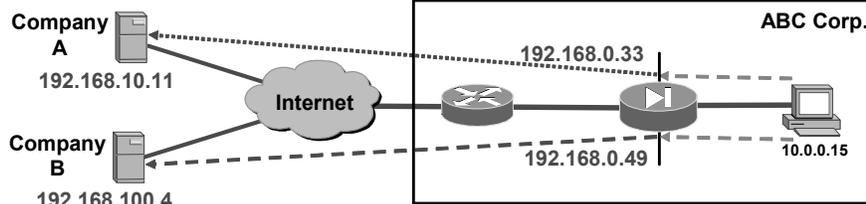
```
pix1(config)# access-list company_a permit tcp 10.0.0.0
  255.255.255.0 host 192.168.10.11 eq www
pix1(config)# nat (inside) 10 access-list company_a
pix1(config)# global (outside) 10 192.168.0.33 netmask
  255.255.255.255
pix1(config)# access-list company_b permit tcp 10.0.0.0
  255.255.255.0 host 192.168.100.4 eq www
pix1(config)# nat (inside) 11 access-list company_b
pix1(config)# global (outside) 11 192.168.0.49 netmask
  255.255.255.255
```

SNPA v4.0—5-25

Policy NAT enables you to identify local traffic for address translation by specifying the source and destination addresses in an extended ACL. With policy NAT, you can create multiple-policy NAT statements based on unique source-port and destination-port combination ACL statements. You can then match different mapped addresses to each source-port and destination-port pair. In the figure, a host on the ABC Corporation network is accessing order entry servers for two different companies. When the ABC Corporation host accesses the Company A order entry server at 192.168.10.11, the ABC Corporation host source address is translated to 192.168.0.33. When the ABC Corporation host accesses the Company B server at 192.168.100.4, the ABC Corporation host source address is translated to 192.168.0.49. To accomplish this, a **nat access-list** command is configured. The ACL defines the source and destination addresses and optional ports, for example, **access-list company_a permit tcp 10.0.0.0 255.255.255.0 host 192.168.10.11 eq www**. The ACL identifies any traffic between the ABC Corporation inside network and the Company A order entry server, 192.168.10.11. The ACL is then applied to a NAT statement, **nat (inside) 10 access-list company_a**. When a packet traversing the security appliance matches the NAT ACL statement, the security appliance translates the source address according to the corresponding **global** statement, **global (outside) 10 192.168.0.33 255.255.255.255**.

In this scenario, a host on the ABC Corporation inside network is translated to a different source address depending on which destination order entry server the packet is being sent to. If the packet is sent to the Company A order entry server, the packet source address is 192.168.0.33. If a packet is sent to the Company B order entry server, the packet is translated to 192.168.0.49. The ACL identifies the traffic flow. The NAT ACL identifies the translated source address.

The syntax of the **nat access-list** command is as follows:

```
nat (real_ifc) nat_id access-list access_list_name
```

real_if	Name of the network interface as specified by the **nameif** command through which the hosts or network that are designated by *real_ip* are accessed.
access-list *access_list_name*	Identifies the local addresses and destination addresses using an extended access list, also known as policy NAT. Create the access list using the **access-list** command. This access list should include only permit access control entries (ACEs). You can optionally specify the local and destination ports in the access list using the **eq** operator. If the NAT ID is 0, then the access list specifies addresses that are exempt from NAT. NAT exemption is not the same as policy NAT; you cannot specify the port addresses, for example.
nat_id	ID of the group of host or networks. It is referenced by the **global** command to associate a global pool with the *real_ip*. Specifies an integer between 1 and 65535. The NAT ID must match a **global** statement NAT ID. 0 is reserved for NAT exemption. A *nat_id* of 0 indicates that no address translation takes place for *real_ip*.
	A *nat_id* of **0 access list** *access_list_name* specifies the traffic to exempt from NAT processing, based on the access list that is specified by the *access_list_name*. This command is useful in a VPN configuration where traffic between private networks should be exempted from NAT

Other Commands Plus ACL

Cisco.com

Corporate office

Branch office

VPN

Internet
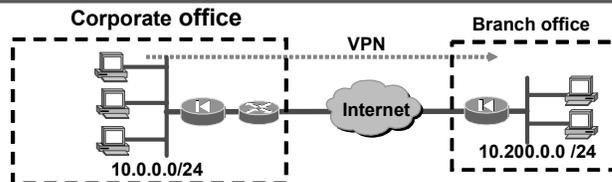
10.0.0.0/24

10.200.0.0 /24

• **Identify traffic (ACL) to be encrypted**
  • **access-list 101** permit ip 10.0.0.0 255.255.255.0 10.200.0.0 255.255.255.0
  •**crypto map** FW1MAP 10 **match address 101**

Web server

Internet
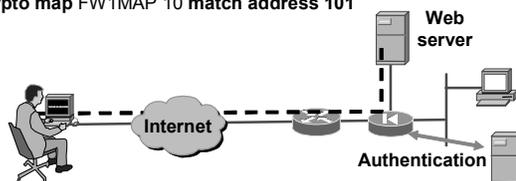
Authentication

• **Identify traffic (ACL) to be authenticated**
  • **access-list 110** permit tcp any host 192.168.2.10 eq www
  • **aaa authentication match 110** outside NY_ACS

SNPA v4.0—5-26

access-list commands can be combined with other commands. In each case, the **access-list** command identifies a traffic flow. The command associates an action with the identified flow of traffic. In the top example in the figure, the administrator identifies a flow of traffic between two sites to be encrypted. The **crypto map** command uses the ACL to differentiate the traffic that is to be protected by encryption from the traffic that does not need protection. Traffic permitted by the ACL is protected.

In the bottom example in the figure, the administrator wants to authenticate certain Internet sourced hosts when they attempt to connect to protected hosts on the DMZ. The traffic is identified with the **access-list 110 permit tcp any host 192.168.2.10 eq www** command. The ACL identifies any host trying to access host 192.168.2.10 using HTTP. Authentication is applied to this flow with the **aaa authentication match 110 outside NY_ACS** command. Any hosts matching ACL 110 will be authenticated.

Malicious Active Code Filtering

The security appliance can filter malicious active codes. Malicious active codes can be used in such applications as Java and ActiveX.

Java Applet Filtering

- **Java applet filtering enables an administrator to prevent the downloading of Java applets by an inside system.**
- **Java programs can provide a vehicle through which an inside system can be invaded.**
- **Java applets are executable programs that are banned within some security policies.**

SNPA v4.0—5-28

Java filtering enables an administrator to prevent Java applets from being downloaded by an inside system. Java applets are executable programs that are banned by many site security policies.

Java programs can provide a vehicle through which an inside system can be invaded or compromised. Java applets can be downloaded when you permit access to HTTP port 80, and some Java applets can contain hidden code that can destroy data on the internal network.

The Java applet filter of Cisco security appliances can stop Java applications on a per-client or per-IP-address basis. When Java filtering is enabled, the security appliance searches for the programmed "café babe" string, and if found, it drops the Java applet. This is a sample Java class code snippet:

```
00000000: café babe 003 002d 0099 0900 8345 0098
```

ActiveX Blocking

- **ActiveX controls are applets that can be inserted in web pages or other applications.**
- **ActiveX controls can provide a way for someone to attack servers.**
- **The security appliance can be used to block ActiveX controls.**

SNPA v4.0—5-29

ActiveX controls, formerly known as Object Linking and Embedding (OLE) controls, are applets—often used in animations— that can be inserted in web pages or in other applications. ActiveX controls create a potential security problem because they can provide a way for someone to attack servers. You can use your security appliance to block all ActiveX controls.

```
fw1(config)# filter activex
 80 0.0.0.0 0.0.0.0 0.0.0.0
 0.0.0.0
```

- **Specifies that the ActiveX blocking applies to web traffic on port 80 from any local host and for connections to any foreign host**

Internet

Block ActiveX

DMZ

Engineering
10.0.11.0

Marketing
10.0.12.0

Executive
10.0.14.0
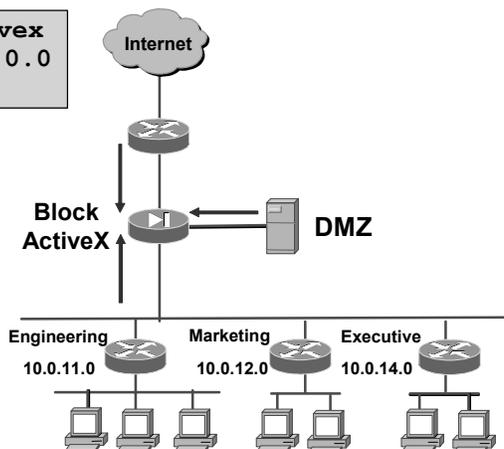
SNPA v4.0—5-30

The **filter** command enables or disables outbound URL or HTML filtering. In the figure above, the command specifies that ActiveX is being filtered on port 80 from any internal host and for connection to any external host.

The **filter** {**activex** | **java**} command filters out ActiveX or Java usage from outbound packets.

The syntax for the **filter** {**activex** | **java**} command is as follows:

```
filter {activex | java} port [-port] local_ip mask foreign_ip
mask
```

activex	Blocks outbound ActiveX and other HTML <object> tags from outbound packets.
java	Blocks Java applets returning from an outbound connection.
port	The port(s) at which Internet traffic is received on the security appliance.
local_ip	The IP address of the host from which access is sought.
mask	Subnet mask.
foreign_ip	The IP address of the host to which access is sought.

URL Filtering

This topic discusses how to configure Cisco security appliances for URL filtering.
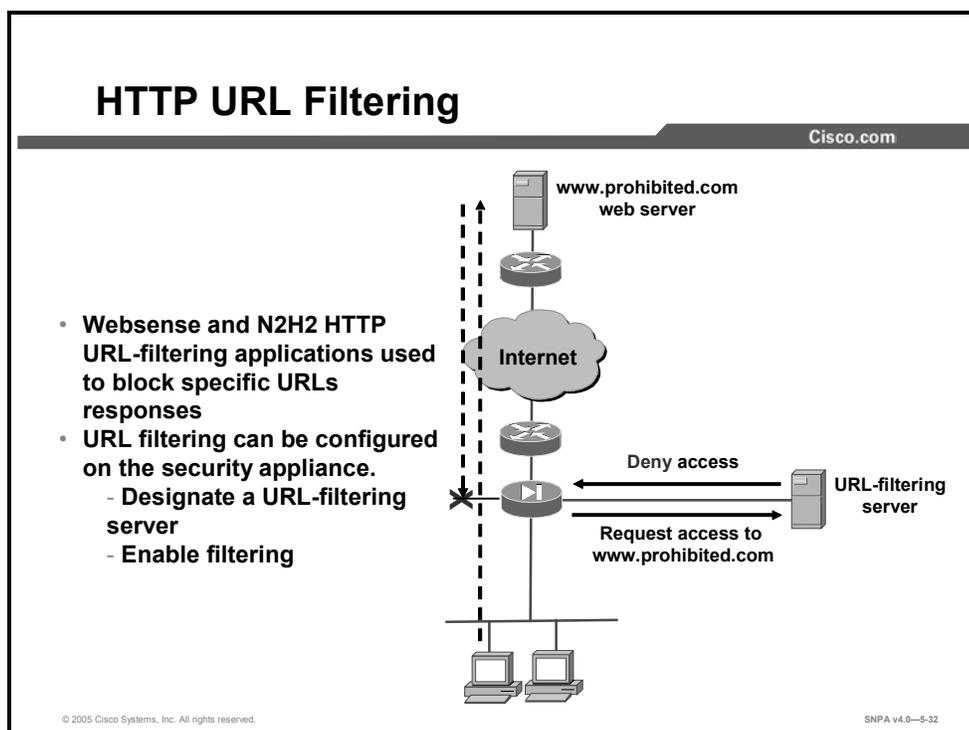
URL-filtering applications provide URL filtering for the security appliance, enabling network administrators to effectively monitor and control network traffic. URL-filtering applications are used to block specific URLs because the security appliance cannot. The security appliance can be enabled to work with the Websense and N2H2 URL-filtering applications. This is useful because between the hours of 9 a.m. and 5 p.m.:

- 30 to 40 percent of Internet surfing is not business-related
- 70 percent of all Internet porn traffic occurs
- More than 60 percent of online purchases are made

When the security appliance receives a request from a user to access a URL, it queries the URL-filtering server to determine whether to return, or block, the requested web page. The URL-filtering server checks its configurations to determine whether the URL should be blocked. If the URL should be blocked, URL-filtering applications can display blocking messages or direct the user that is requesting the URL to a specified web site.

Information about Websense, N2H2, and other Cisco Partners is available at Cisco.com.

Designate the URL-Filtering Server

Cisco.com
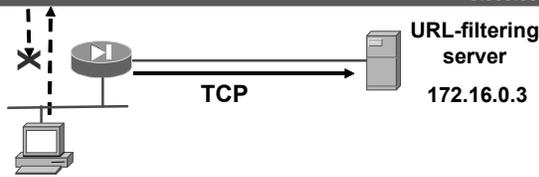
URL-filtering
server

TCP

172.16.0.3

firewall(config)#

```
url-server [(if_name)] [vendor websense] host local_ip
  [timeout seconds] [protocol {TCP | UDP} version [1 | 4]]
```

• **Designates a server that runs a Websense URL-filtering application**

firewall(config)#

```
url-server [(if_name)] vendor n2h2 host local_ip [port
  number][timeout seconds][protocol {TCP | UDP}]
```

• **Designates a server that runs an N2H2 URL-filtering application**

```
fw1(config)# url-server (dmz) vendor n2h2 host
  172.16.0.3 protocol TCP
```

SNPA v4.0—5-33

Before you can begin URL filtering, you must designate at least one server on which the Websense or N2H2 URL-filtering application will run. The limit is 16 URL servers. You can use only one application at a time, either N2H2 or Websense. Additionally, changing your configuration on the security appliance does not update the configuration on the application server; this must be done separately, according to the instructions of the vendor.

Use the **url-server** command to designate the server on which it runs, then enable URL filtering with the **filter url** command.

The syntax for the **url-server** command as used with Websense is as follows:

```
url-server [(if_name)] vendor websense host local_ip [timeout
seconds] [protocol {TCP | UDP | connections num_conns] |
version]
```

connections	Limits the maximum number of connections permitted.
if_name	The network interface where the authentication server resides. If not specified, the default is inside.
host local_ip	The server that runs the URL-filtering application.
timeout seconds	The maximum idle time that is permitted before the security appliance switches to the next server that you specified. The default is 5 seconds.
protocol	The protocol can be configured using **TCP** or **UDP** keywords. The default is TCP v1.
vendor websense	Indicates URL filtering service vendor is Websense.
version	Specifies protocol version, **1** or **4**. The default is TCP v1. TCP can be configured using Release 1 or Release 4. UDP can be configured using Release 4 only.

The syntax for the url-server command as used with N2H2 is as follows:

```
url-server [(if_name)] vendor n2h2 host local_ip [port number]
[timeout seconds] [protocol {TCP | UDP [connections
num_conns]}]
```

connections	Limits the maximum number of connections permitted.
num_conns	Specifies the maximum number of connections permitted.
host *local_ip*	The server that runs the URL filtering application.
if_name	(Optional)The network interface on which the authentication server resides. If not specified, the default is inside.
port *number*	The N2H2 server port. The security appliance also listens for UDP replies on this port. The default port number is 4005.
protocol	The protocol can be configured using **TCP** or **UDP** keywords. The default is TCP.
timeout *seconds*	The maximum idle time permitted before the security appliance switches to the next server you specified. The default is 5 seconds.
vendor n2h2	Indicates URL-filtering application vendor is N2H2.

Enable HTTP URL Filtering

Cisco.com

Filter HTTP: all hosts

URL-filtering server
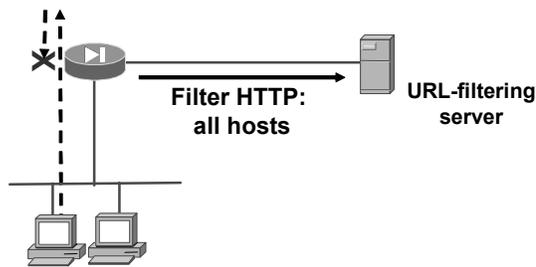
firewall(config)#

```
filter url [http | port[-port]] local_ip local_mask
  foreign_ip foreign_mask [allow]
```

• **Prevents users from accessing URLs that are designated with the URL-filtering application**

```
fw1(config)# filter url http 0 0 0 0 allow
```

SNPA v4.0—5-34

After designating which server runs the URL-filtering application, use the **filter url** command to tell the security appliance to send URL requests to that server for filtering.

The example in the figure above instructs the security appliance to send all URL requests to the URL-filtering server to be filtered. The **allow** option in the **filter** command is crucial to the use of the security appliance URL filtering feature. If you use the **allow** option and the URL-filtering server goes offline, the security appliance lets all URL requests continue without filtering. If the **allow** option is not specified, all port 80 URL requests are stopped until the server is back online.

The syntax for the **filter url** command is as follows:

```
filter url {[port[-port] | except } local_ip local_mask
foreign_ip foreign_mask] [allow] [cgi-truncate] [longurl-
truncate | longurl-deny] [proxy-block]
```

url	Filters URLs from data that is moving through the security appliance.
port	The port that receives Internet traffic on the security appliance. Typically, this is port 80, but other values are accepted. The HTTP or URL literal can be used for port 80.
except	Creates an exception to a previous filter condition.
local_ip	The IP address of the host from which access is sought.
local_mask	Network mask of *local_ip*.
foreign_ip	The IP address of the host to which access is sought.
foreign_mask	Network mask of *foreign_ip*.
allow	Enables outbound connections to pass through the security appliance without filtering when the URL-filtering server is unavailable.
proxy-block	Prevents users from connecting to an HTTP proxy server.

longurl-truncate	Enables outbound URL traffic whether or not the URL buffer is available.
longurl-deny	Denies the URL request if the URL is over the URL buffer size limit or if the URL buffer is not available.
cgi-truncate	Sends a Common Gateway Interface (CGI) script as a URL.

HTTPS and FTP Filtering

Cisco.com

HTTPS and FTP
filtering
(Websense only)

URL-filtering
server
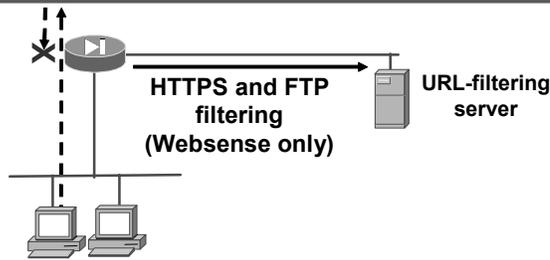
firewall(config)#

```
filter [ https | ftp ] dest-port] local_ip local_mask
  foreign_ip foreign_mask [allow]
```

• **Prevents users from accessing HTTPS and FTP URLs that are designated with the Websense-based URL-filtering application**

```
fw1(config)# filter https 0 0 0 0 allow
```

SNPA v4.0—5-35

This feature extends web-based URL filtering to HTTPS and File Transfer Protocol (FTP). The **filter ftp** and **filter https** commands were added to the **filter** command in Cisco PIX Security Appliance Software v6.3. The **filter ftp** command enables FTP filtering. The **filter https** command enables HTTPS filtering. The **filter ftp** and **filter https** commands are available with Websense URL filtering only.

The example command in the figure instructs the security appliance to send all URL requests to the URL-filtering server to be filtered. The **allow** option in the **filter** command is crucial to the use of the security appliance URL-filtering feature. If you use the **allow** option and the URL-filtering server goes offline, the security appliance lets all FTP and HTTPS URL requests continue without filtering. If the **allow** option is not specified, all FTP and HTTPS URL requests are stopped until the server is back online.

The syntax for the **filter https** command is as follows:

```
filter https {[port[-port] | except } local_ip local_mask
foreign_ip foreign_mask] [allow]
```

port	The TCP port to which filtering is applied. Typically, this is port 443, but other values are accepted. The HTTPS literal can be used for port 443.
port-port	(Optional) Specifies a port range.
except	(Optional) Creates an exception to a previous filter condition.
dest-port	The destination port number.
local_ip	The IP address of the highest security level interface from which access is sought. You can set this address to **0.0.0.0** (or, in shortened form, **0**) to specify all hosts.
local_mask	Network mask of *local_ip*. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.

foreign_ip	The IP address of the lowest security level interface to which access is sought. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
foreign_mask	Network mask of *foreign_ip*. Always specify a mask value. You can use **0.0.0.0** (or, in shortened form, **0**) to specify all hosts.
allow	(Optional) When the server is unavailable, let outbound connections pass through the security appliance without filtering. If you omit this option and the N2H2 or Websense server goes offline, the security appliance stops outbound port 443 traffic until the N2H2 or Websense server is back online.

The syntax for the **filter ftp** command is as follows:

```
filter ftp {[port[-port] | except } local_ip local_mask
foreign_ip foreign_mask] [allow] [interact-block]
```

port	The TCP port to which filtering is applied. Typically, this is port 443, but other values are accepted. The HTTP literal can be used for port 443.
port-port	(Optional) Specifies a port range.
except	(Optional) Creates an exception to a previous filter condition.
local_ip	The IP address of the highest security level interface from which access is sought. You can set this address to **0.0.0.0** (or, in shortened form, **0**) to specify all hosts.
local_mask	Network mask of *local_ip.* You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
foreign_ip	The IP address of the lowest security level interface to which access is sought. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
foreign_mask	Network mask of *foreign_ip*. Always specify a mask value. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
allow	(Optional) When the server is unavailable, let outbound connections pass through the security appliance without filtering. If you omit this option and the N2H2 or Websense server goes offline, the security appliance stops outbound port 443 traffic until the N2H2 or Websense server is back online.
interact-block	(Optional) Prevents users from connecting to the FTP server through an interactive FTP program.

URL Filtering Configuration Example

www.prohibited.com
web server

Internet

```
fw1(config)# url-server (dmz) vendor
  websense host 172.16.0.3 timeout 10
  protocol TCP version 4
fw1(config)# filter url http 0 0 0 0 allow
```

• **Designate URL server**
• **Enable filtering**

Deny access

URL-filtering
server
172.16.0.3

Request access to
www.prohibited.com

SNPA v4.0—5-36
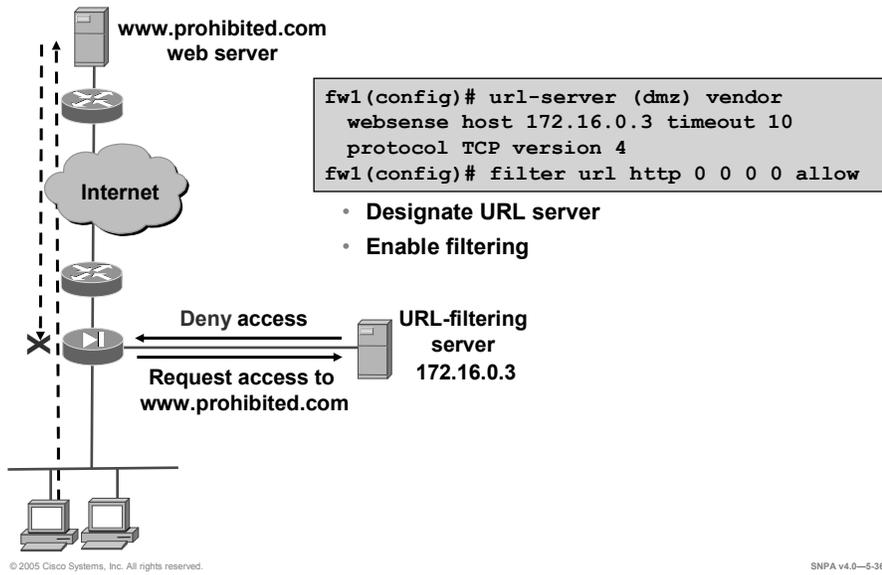
The commands in the figure instruct the security appliance to send all URL requests to the Websense URL-filtering server at 172.16.0.3. Additionally, if the URL-filtering server goes offline, the security appliance allows all URL requests to continue without filtering.

Summary

This topic summarizes the information you learned in this lesson.

Summary

- **ACLs enable you to determine which systems can establish connections through your security appliance.**
- **With ICMP ACLs, you can disable pinging to a security appliance interface so that your security appliance cannot be detected on your network.**
- **The security appliance can be configured to filter malicious active code.**
- **The security appliance can work with URL-filtering software to control and monitor Internet activity.**

SNPA v4.0—5-37

Lesson 6

Object Grouping

Overview

This lesson introduces object grouping concepts and how to use the **object-group** command to configure object grouping. The lesson also explains the various types of object groups and covers the uses and configurations of nested object groups.

Objectives

Upon completing this lesson, you will be able to describe and configure the object grouping feature of Cisco security appliances. This includes being able to meet these objectives:

- Describe the object grouping feature of the security appliance and its advantages

- Configure object groups

- Configure nested object groups

- Use object groups in ACLs

Overview of Object Grouping

This topic introduces the concepts of object grouping.

Using Object Groups in ACLs

```
fw1(config)# show run static
static (dmz,outside) 192.168.0.10
   172.16.0.1 netmask 255.255.255.255
static (dmz,outside) 192.168.0.11
   172.16.0.2 netmask 255.255.255.255
static (dmz,outside) 192.168.0.12
   172.16.0.3 netmask 255.255.255.255
```

```
fw1(config)# access-list acl_out permit tcp any
   host 192.168.0.10 eq http
fw1(config)# access-list acl_out permit tcp any
   host 192.168.0.10 eq https
fw1(config)# access-list acl_out permit tcp any
   host 192.168.0.10 eq ftp
fw1(config)# access-list acl_out permit tcp any
   host 192.168.0.11 eq http
fw1(config)# access-list acl_out permit tcp any
   host 192.168.0.11 eq https
fw1(config)# access-list acl_out permit tcp any
   host 192.168.0.11 eq ftp
fw1(config)# access-list acl_out permit tcp any
   host 192.168.0.12 eq http
fw1(config)# access-list acl_out permit tcp any
   host 192.168.0.12 eq https
fw1(config)# access-list acl_out permit tcp any
   host 192.168.0.12 eq ftp
```

Internet

192.168.0.X

DMZ

172.16.0.0

Web .1

Web .2

Web .3

SNPA v4.0—6-3

An access control list (ACL) can cause a security appliance to allow a designated client to access a particular server for a specific service. When there is only one client, one host, and one service, only a minimum number of lines is needed in an ACL. However, as the number of clients, servers, and services increases, the number of lines that are required in an ACL increases exponentially.

In the figure, the Internet hosts are granted Hypertext Transfer Protocol (HTTP), HTTP secure (HTTPS), and File Transfer Protocol (FTP) access to specific hosts on the demilitarized zone (DMZ). An ACL is configured for each individual host and protocol combination. There are three hosts, three protocols, and nine lines in the ACL.

Grouping Objects

```
fw1(config)# show run static
static(dmz,outside)192.168.0.10
  172.16.0.1 netmask 255.255.255.255
static(dmz,outside)192.168.0.11
  172.16.0.2 netmask 255.255.255.255
static(dmz,outside)192.168.0.12
  172.16.0.3 netmask 255.255.255.255
```

- **Services groups, such as DMZ_Services**
  - **HTTP**
  - **HTTPS**
  - **FTP**
- **Host and network groups, such as DMZ_Servers**
  - **192.168.0.10**
  - **192.168.0.11**
  - **192.168.0.12**
- **Group names applied to ACL**
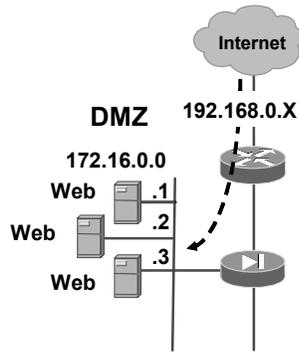
Internet

DMZ **192.168.0.X**

172.16.0.0

Web .1

Web .2

.3

Web

```
fw1(config)# access-list outside permit tcp any
  object-group DMZ_Servers object-group
  DMZ_Services
```

You can group network objects such as hosts and services to simplify the task of creating and applying ACLs. This reduces the number of access control entries (ACEs) that are required to implement complex security policies. For example, a security policy that normally contains 3,300 ACEs within an ACL might require only several hundred ACEs within that ACL after hosts and services are properly grouped.

Applying a security appliance object group to a security appliance command is the equivalent of applying every element of the object group to the command. For example, the group DMZ_Servers contains servers 192.168.0.10, 192.168.0.11, and 192.168.0.12. The group DMZ_Services supports HTTP, HTTPS, and FTP protocols. Applying the groups DMZ_Servers and DMZ_Services to an ACE is the same as applying all the individual hosts and protocols to the ACE. Therefore, the command:

```
access-list outside permit tcp any object-group DMZ_Servers
object-group DMZ_Services
```

is equivalent to the following:

```
fw1(config)# access-list outside permit tcp any host
192.168.0.10 eq http
fw1(config)# access-list outside permit tcp any host
192.168.0.10 eq https
fw1(config)# access-list outside permit tcp any host
192.168.0.10 eq ftp
fw1(config)# access-list outside permit tcp any host
192.168.0.11 eq http
fw1(config)# access-list outside permit tcp any host
192.168.0.11 eq https
fw1(config)# access-list outside permit tcp any host
192.168.0.11 eq ftp
fw1(config)# access-list outside permit tcp any host
192.168.0.12 eq http
fw1(config)# access-list outside permit tcp any host
192.168.0.12 eq https
fw1(config)# access-list outside permit tcp any host
192.168.0.12 eq ftp
```

Grouping Objects of Similar Types

- **Protocols**
  - **TCP**
  - **UDP**

- **INSIDE_PROTOCOLS**

- **Networks and hosts**
  - **Subnet 10.0.0.0/24**
  - **10.0.1.11**
  - **10.0.2.11**

- **INSIDE_HOSTS**
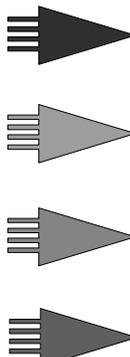
- **Services**
  - **HTTP**
  - **HTTPS**
  - **FTP**

- **DMZ_SERVICES**

- **ICMP**
  - **Echo**
  - **Echo-reply**

- **PING**

Protocols **Networks/Hosts** **Services/ ICMP**

firewall(config)# access-list aclout permit tcp any host 192.168.0.12 eq ftp
firewall(config)# access-list aclout permit icmp any 192.168.0.12 echo-reply

SNPA v4.0—6-5

Object grouping provides a way to group objects of a similar type so that a single ACE can apply to all the objects in the group. You can create the following types of object groups:

- Network: Used to group client hosts, server hosts, or subnets.

- Protocol: Used to group protocols. It can contain one of the keywords **icmp**, **ip**, **tcp**, or **udp** or an integer in the range 1 through 254 representing an IP protocol number. Use the keyword **ip** to match any Internet protocol, including ICMP, TCP, and User Datagram Protocol (UDP).

- Service: Used to group TCP or UDP port numbers assigned to a different service.

- ICMP-type: Used to group ICMP message types to which you permit or deny access.

Getting Started with Object Groups

This topic explains the **object-group** command and its subcommand mode.

Configuring and Using Object Groups

Cisco.com

Complete the following steps to create object groups and use them in your configuration:

- **Step 1: Use the** object-group **command to enter the appropriate subcommand mode for the type of group you want to configure.**
- **Task 2: In subcommand mode, define the members of the object group.**
- **Task 3: (Optional) Use the** description **subcommand to describe the object group.**
- **Task 4: Use the** exit **or** quit **command to return to configuration mode.**
- **Task 5: (Optional) Use the** show object-group **command to verify that the object group has been configured successfully.**
- **Task 6: Apply the object group to the** access-list **command.**
- **Task 7: (Optional) Use the** show access-list **command to display the expanded ACL entries.**

© 2005 Cisco Systems, Inc. All rights reserved.   SNPA v4.0—6-7

Complete the following steps to configure an object group and to use it for configuring ACLs:

Step 3   Use the **object-group** command to enter the appropriate subcommand mode for the type of group you want to configure. When you enter the **object-group** command, the system enters the appropriate subcommand mode for the type of object you specify in the **object-group** command. All subcommands entered from the subcommand prompt apply to the object group identified by the **object-group** command.

Step 4   In subcommand mode, define the members of the object group. In subcommand mode, you can enter object grouping subcommands as well as all other security appliance commands, including **show** commands and **clear** commands. Enter a question mark (?) in the subcommand mode to view the permitted subcommands.

Step 5   (Optional) Use the **description** subcommand to describe the object group.

Step 6   Return to configuration mode with the **exit** command or the **quit** command. When you enter any valid configuration command other than one designed for object grouping, the subcommand mode is terminated.

Step 7   (Optional) Use the **show run object-group** command to verify that the object group has been configured successfully. This command displays a list of the currently configured object groups of the specified type. Without a parameter, the command displays all object groups.

Step 8   Apply the object group to the **access-list** command. Replace the parameters of the **access-list** commands with the corresponding object group, as summarized by the following:

■ Replace the protocol parameter with one protocol object group preceded by the keyword **object-group**.

■ Replace the source IP address and subnet mask with one network object group preceded by the keyword **object-group**.

■ Replace the destination IP address and subnet mask with one network object group preceded by the keyword **object-group**.

■ Replace the port parameter with one service object group preceded by the keyword object-group.

■ Replace the *icmp-type* parameter with one ICMP-type object group preceded by the keyword **object-group**.

For example, the following command enables access for the members of the network object group DMZHosts:

```
access-list EXAMPLE permit tcp any object-group DMZHosts
```

Step 9   (Optional) Use the **show access-list** command to display the expanded ACEs.

Configuring Object Groups

This topic explains how to configure network, service, protocol, and ICMP-type object groups.

Configuring Network Object Groups

Cisco.com

10.0.0.0 /24

Inside_Eng

Internet

192.168.0.0

Inside_Mktg

10.0.1.0/24

firewall(config)#

```
object-group {protocol | network | icmp-type}
    obj_grp_id
```

* **Assigns a name to the group and enables the network subcommand mode**

```
fw1(config)# object-group network Inside_Eng
fw1(config-network)# network-object host 10.0.0.1
fw1(config-network)# network-object host 10.0.0.2
```

SNPA v4.0—6-8

To configure a Network object group, first enter the **object-group network** command to name the network object group and enable the network object subcommand mode. After you are inside the subcommand mode, you can use the **network-object** command to add a single host or network to the network object group.

The syntax for the **network-object** command is as follows:

```
network-object host host_addr | host_name
network-object net_addr netmask
```

host	Keyword used with the *host_addr* parameter to define a host object.
host-addr	Host IP address (if the host name is not already defined using the **name** command).
host_name	Host name (if the host name is defined using the **name** command).
net_addr	Network address; used with *netmask* to define a subnet object.
netmask	Netmask; used with *net_addr* to define a subnet object.

In the figure, the administrator wants to add specific 10.0.0.0/24 hosts to the Inside_Eng object group. The object group Inside_Eng is defined first. In the subcommand mode, the individual hosts are added to the group, hosts 10.0.0.1 and 10.0.0.2.

Configuring Service Object Groups

Cisco.com

Host_Services
- **HTTP**
- **HTTPS**
- **FTP**

Internet

192.168.0.0

Inside_Eng

10.0.0.0 /24

Inside_Mktg

10.0.1.0/24
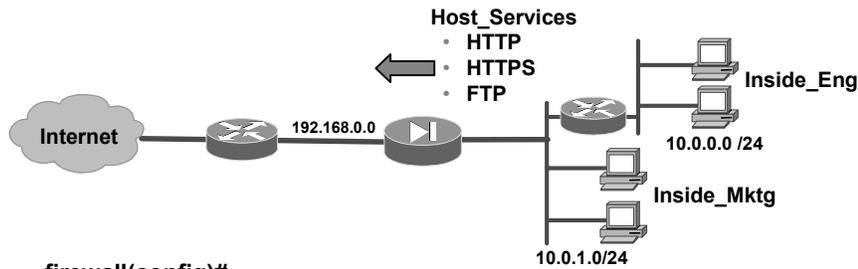
firewall(config)#

```
object-group service obj_grp_id {tcp | udp | tcp-udp}
```

- **Assigns a name to a service group and enables the service subcommand mode**

```
fw1(config)# object-group service Host_Services tcp
fw1(config-service)# port-object eq http
fw1(config-service)# port-object eq https
fw1(config-service)# port-object eq ftp
```

SNPA v4.0—6-9

To configure a service object group, first enter the **object-group service** command to name the service object group and enable the service subcommand mode. Using the **tcp** option specifies that the service object group contains ports that are used for TCP only. Using the **udp** option specifies that the service object group contains ports that are used for UDP only. Using the **tcp-udp** option specifies that the service object group contains ports that are used for both TCP and UDP.

After you're inside the subcommand mode, you can use the **port-object** command to add a TCP or UDP port number to the service object group. You can also add a range of TCP or UDP port numbers to the service object group.

The syntax for the **port-object** commands is as follows:

```
port-object eq service
port-object range begin_service end_service
```

eq *service*	Specifies the decimal number or name of a TCP or UDP port for a service object.
range	Specifies a range of ports (inclusive).
begin_service	Specifies the decimal number or name of a TCP or UDP port that is the beginning value for a range of services. This value must be between 0 and 65535.
end_service	Specifies the decimal number or name of a TCP or UDP port that is the ending value for a range of services. This value must be between 0 and 65535.

In the figure, the administrator wants each Inside_Eng host to have outbound HTTP, HTTPS, and FTP capabilities. A service object group, Host_Services, is defined. Individual protocols, HTTP, HTTPS, and FTP, are added in the subcommand mode.

Note	The protocol type of a service group object and the protocol type of the ACE to which it is associated must match. For example, if the service object group Host_Services is created for TCP services, this object can only be associated with an ACE (permit or deny) that also refers to TCP services as in the following example:

```
firewall(config)# access-list inside permit tcp object-group
Inside_Eng any object-group Host_Services
```

Adding Object Groups to an ACL
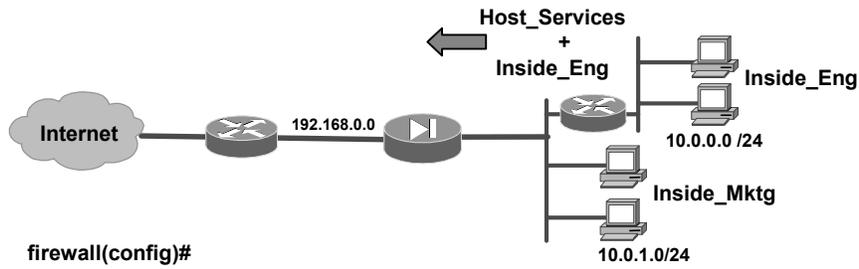
**Host_Services
+
Inside_Eng**

Inside_Eng

Internet

192.168.0.0

10.0.0.0 /24

Inside_Mktg

firewall(config)#

10.0.1.0/24

```
access-list id [line line-number] [extended] {deny | permit}
{protocol | object-group protocol_obj_grp_id}{host sip | sip mask |
  interface ifc_name | object-group network_obj_grp_id | any}{host
  dip | dip mask | interface ifc_name | object-group
  network_obj_grp_id | any}[log [[level] [interval secs] | disable |
  default]][inactive | time-range time_range_name]
```

- **Permits outbound engineering HTTP, HTTPS, and FTP traffic**

```
fw1(config)# access-list inside permit tcp object-group Inside_Eng any object-
group Host_Services
```

The last step is to add the object groups to an ACL. In the figure, Inside_Eng and Host_Services are defined within the ACL statement. Hosts within the Inside_Eng group can access outbound any host with the protocols defined within the Host_Services object group.

The following is the syntax for the **protocol-object** command:

```
protocol-object protocol
```

protocol	Protocol name or number.

Configuring ICMP-Type Object Groups

```
firewall(config)#
```
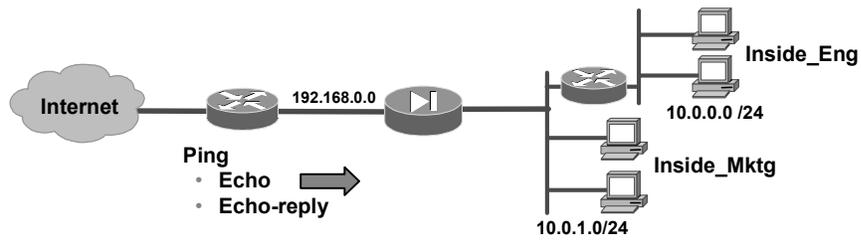
```
object-group icmp-type obj_grp_id
```

- **Assigns a name to an ICMP-type group and enables the ICMP-type subcommand mode**

```
fw1(config)# object-group icmp-type PING
fw1(config-icmp)# icmp-object echo
fw1(config-icmp)# icmp-object echo-reply
```

SNPA v4.0—6-11

To configure an ICMP-type object group, first enter the **object-group icmp-type** command to name the ICMP-type object group and enable the ICMP-type subcommand mode. After you are inside the subcommand mode, you can use the **icmp-object** command to add an ICMP message type to the object group.

The syntax for the **icmp-object** command is as follows:

```
icmp-object icmp-type
```

| *icmp-type* | Specifies an ICMP message type. |

The following are valid ICMP message types:

- 0: echo-reply
- 3: destination-unreachable
- 4: source-quench
- 5: redirect
- 6: alternate-address
- 8: echo
- 9: router-advertisement
- 10: router-solicitation
- 11: time-exceeded
- 12: parameter-problem
- 13: timestamp-request
- 14: timestamp-reply
- 15: information-request

- 16: information-reply
- 17: address-mask-request
- 18: address-mask-reply
- 31: conversion-error
- 32: mobile-redirect

Nested Object Groups

This topic explains how to configure and use nested object groups.
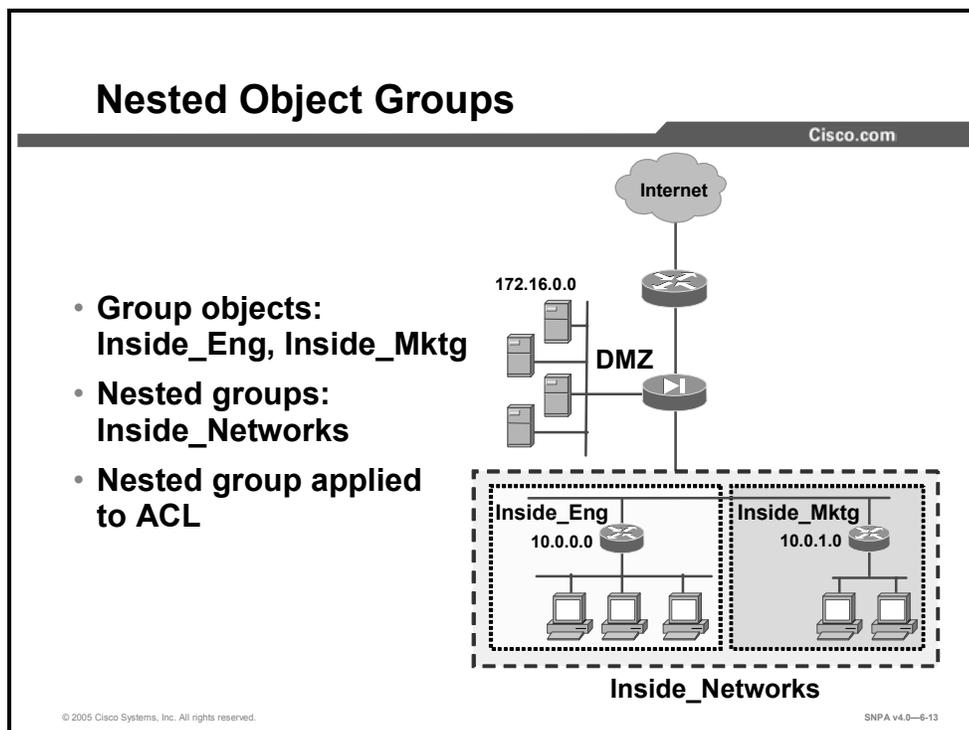
You learned how to group objects to simplify the task of creating and applying ACLs. It is also possible to group objects within a nested group. An object can be a member of a group. For object groups to be nested, they must be of the same type, for example, all networks and hosts. In the figure, the administrator configured hosts from the 10.0.0.0/24 network to form the Inside_Eng object group. The administrator added hosts from the 10.0.1.0/24 network to form the Inside_Mktg object group. For some ACLs, the administrator found it advantageous to combine the Inside_Eng and Inside_Mktg object groups to form the nested object group Inside_Networks and apply that nested object group to selected ACLs. Hierarchical object grouping can achieve greater flexibility and modularity for specifying access rules.

The **group-object** command enables you to construct hierarchical, or nested, object groups. The difference in object groups and group objects is as follows:

■ An object group is a group consisting of objects.

■ A group object is an object in a nested group and is itself a group.

Duplicated objects are allowed in an object group if it is a result of the inclusion of group objects. For example, if object 1 is in both group A and group B, you can define a group C which includes both A and B. You cannot, however, include a group object, which causes the group hierarchy to become circular. For example, you cannot have group A include group B and also have group B include group A.

Configuring Nested Object Groups

Complete the following steps to configure nested object groups:

- **Step 1: Create an object group, such as Inside_Eng that you want to nest within another object group.**
- **Step 2: Add the appropriate type of objects to the object group, such as 10.0.1.0/24.**
- **Step 3: Assign an identity, such as Inside_Networks to the object group within which you want to nest other object groups.**
- **Step 4: Add the first object group to the second object group.**
- **Step 5: Add any other objects to the group that are required, such as Inside_Mktg.**

Complete the following steps to configure nested object groups:

Step 10 Assign a group identity to the object group that you want to nest within another object group:

```
firewall(config)# object-group network Inside_Eng
```

Step 11 Add the appropriate type of objects to the object group:

```
firewall(config-network)# network-object 10.0.1.0
255.255.255.0
firewall(config-network)# network-object 10.0.2.0
255.255.255.0
firewall(config-network)# network-object 10.0.3.0
255.255.255.0
```

Step 12 Create the object group within which you want to nest another object group:

```
firewall(config)# object-group network Inside_Networks
```

Step 13 Add the first object group to the group that will contain it:

```
firewall(config-network)# group-object Inside_Eng
```

Step 14 Add any other objects that are required to the group:

```
firewall(config-network)# network-object 10.0.4.0
255.255.255.0
```

The resulting configuration of Inside_Networks in this example is equivalent to the following:

```
firewall(config-network)# network-object 10.0.1.0
255.255.255.0
firewall(config-network)# network-object 10.0.2.0
255.255.255.0
firewall(config-network)# network-object 10.0.3.0
255.255.255.0
firewall(config-network)# network-object 10.0.4.0
255.255.255.0
```

Nested Object Group Example: Object Group Network

- **Create object groups**
  - **Inside_Eng**
  - **Inside_Mktg**
- **Allow inside hosts outbound**
  - **HTTP**
  - **HTTPS**
  - **FTP**

Internet

172.16.0.0

DMZ

Inside_Eng
10.0.0.0

Inside_Mktg
10.0.1.0

Inside_Networks
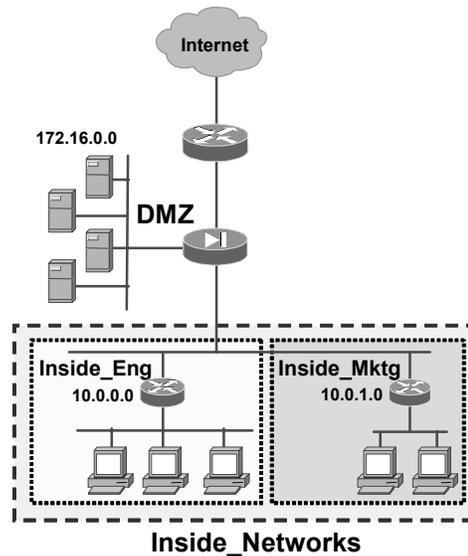
SNPA v4.0—6-15

In the example in the figure, the administrator wants to enable selected hosts to establish HTTP, HTTPS, and FTP outbound sessions. The administrator configures an object group for selected Inside_Eng and Inside_Mktg hosts. These two groups are nested inside another group, Inside_Networks. To ease configuration, the three protocols are grouped.

group-object Command

Cisco.com

Inside_Eng
10.0.0.0

Inside_Mktg
10.0.1.0
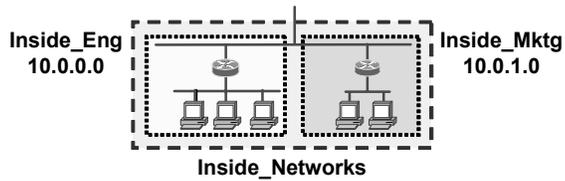
Inside_Networks

`firewall(config-network)#`

```
group-object obj_group_id
```

• **Nests an object group within another object group**

```
fw1(config)# object-group network Inside_Eng
fw1(config-network)# network-object host 10.0.0.1
fw1(config-network)# network-object host 10.0.0.2
fw1(config-network)# exit
fw1(config)# object-group network Inside_Mktg
fw1(config-network)# network-object host 10.0.1.1
fw1(config-network)# network-object host 10.0.1.2
fw1(config-network)# exit
fw1(config)# object-group network Inside_Networks
fw1(config-network)# group-object Inside_Eng
fw1(config-network)# group-object Inside_Mktg
```

　　SNPA v4.0—6-16

The **group-object** command is a subcommand of the **object-group** command and is used to nest an object group within another object group. For object groups to be nested, they must be of the same type. For example, you can group two or more network object groups together, but you cannot group a protocol object group and a network object group together.

The syntax for the **group-object** command is as follows:

```
group-object obj_group_id
```

obj_group_id	Identifies the object group (one to 64 characters) and can be any combination of letters, digits, and the characters "_", "-", and ".".

In the example in the figure, hosts 10.0.0.1 and 10.0.0.2 are grouped into the Inside_Eng object group. Hosts 10.0.1.1 and 10.0.1.2 are grouped into the Inside_Mktg object group. These two object groups are combined into one nested group called Inside_Networks.

Nested Object Group Example: Object Group Services

```
fw1(config)# object-group service Host_Services
   tcp
fw1(config-service)# port-object eq http
fw1(config-service)# port-object eq https
fw1(config-service)# port-object eq ftp
```
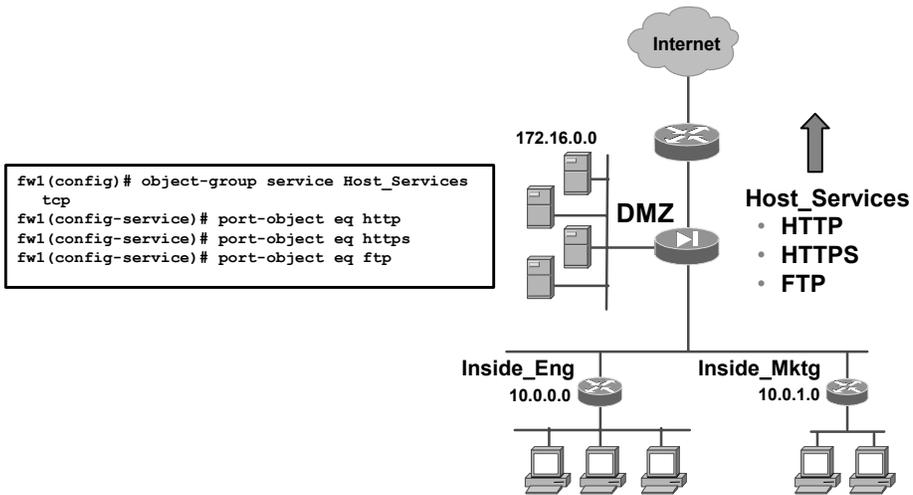
SNPA v4.0—6-17

In the example in the figure, three protocols are combined into one services object group. All the hosts in Inside_Eng and Inside_Mktg have the same protocol privileges. It is easier to group the protocols than to add them to ACLs individually.

Apply Nested Object Group to ACL

Cisco.com

- **Allow all inside hosts outbound**
  - **HTTP**
  - **HTTPS**
  - **FTP**

```
fw1(config)# access-list aclin permit
tcp object-group Inside_Networks any
object-group Host_Services
```

Internet

172.16.0.0

DMZ

Inside_Eng
10.0.0.0

Inside_Mktg
10.0.1.0

Inside_Networks
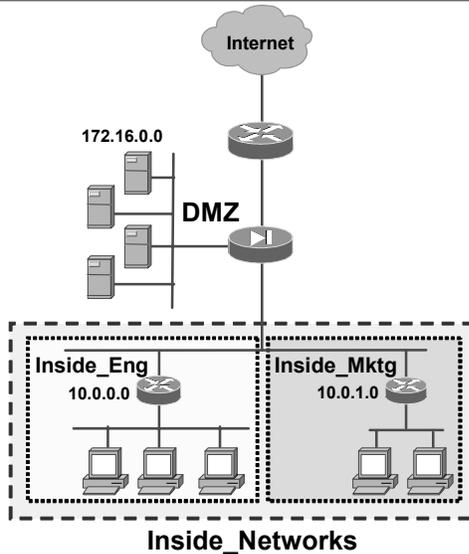
SNPA v4.0—6-18

The keyword **object-group** must precede the object group name in order to use object groups in your ACLs. An object group cannot be removed or emptied if it is currently being used in an ACL command. In the figure, all hosts in the Inside_Networks nested group are permitted to access any host via the services in the Host_Services group.

When used with object grouping, the syntax for the **access-list** commands is as follows:

```
access-list id [line line-number] [extended] {deny | permit}
{tcp | udp} {host sip | sip mask | interface ifc_name |
object-group network_obj_grp_id | any} [operator port] |
object-group service_obj_grp_id] {host dip | dip mask |
interface ifc_name | object-group network_obj_grp_id | any}
[operator port] | object-group service_obj_grp_id] [log
[[level] [interval secs] | disable | default]] [inactive |
time-range time_range_name]

access-list id [line line-number] [extended] {deny | permit}
icmp {host sip | sip mask | interface ifc_name | object-group
network_obj_grp_id | any} {host dip | dip mask | interface
ifc_name | object-group network_obj_grp_id | any} [icmp_type |
object-group icmp_type_obj_grp_id] [log [[level] [interval
secs] | disable | default]] [inactive | time-range
time_range_name]
```

deny	This option does not allow a packet to traverse the security appliance if the conditions are matched. By default, the security appliance denies all inbound or outbound packets unless you specifically permit access.
dip	Specifies the IP address of the network or host to which the packet is being sent. Specify a destination IP address when the **access-list** command statement is used in conjunction with an **access-group** command statement or in conjunction with the **aaa match access-list** command and the **aaa authorization** command. For inbound and outbound connections, the destination IP address is the address before Network Address Translation (NAT) has been performed.
dip_mask	Netmask bits (mask) to be applied to the destination IP address.
icmp_type	(Optional) Specifies the ICMP message type.
icmp_type_obj_grp_id	(Optional) Specifies the identifier of an existing ICMP-type object group.
id	Specifies the name or number of an ACL.
inactive	Disables an access control element
interface *ifc_name*	Specifies the interface address as the source or destination address.
interval *secs*	Specifies the log interval at which to generate a 106100 syslog message; valid values are from 1 to 600 seconds. Default is 300.
line *line-num*	(Optional) The line number at which to insert an access control element.
log disable | default | *level*	(Optional) Specifies that the log option is disabled, set to default values, or set to a syslog level from 0 to 7. The default level is 6. When enabled, a syslog message 106100 is generated for the access control element.
network_obj_grp_id	Specifies the identifier of an existing network object group.
object-group	Specifies an object group.
operator	Compares source IP address or destination IP address ports. Possible operands include "lt" (less than), "gt" (greater than), "eq" (equal), "neq" (not equal), and "range" (inclusive range).
permit	The **permit** option selects a packet to traverse the security appliance if conditions are matched. By default, the security appliance denies all inbound or outbound packets unless you specifically permit access.
port	Specifies the decimal number or name of a TCP or UDP port.
protocol	Specifies the IP protocol name or number that will be open. For example, UDP is 17, TCP is 6, and EGP is 47.
protocol_obj_grp_id	Specifies the identifier of an existing protocol object group.
service_obj_grp_id	Specifies the identifier of an existing service object group.
sip	Specifies the IP address of the network or host from which the packet is being sent.
sip_mask	Netmask bits (mask) to be applied to the source IP address.
time-range *time_range_name*	(Optional) Specifies the time range used to define specific times of the day and week to allow access to the security appliance.

Multiple Object Groups in ACLs

Cisco.com

```
fw1(config)# show run static
static(dmz1,outside)192.168.1.10
   172.16.0.1 netmask 255.255.255.255
static(dmz1,outside)192.168.1.12
   172.16.0.2 netmask 255.255.255.255
static(dmz2,outside)192.168.2.10
   172.16.1.1 netmask 255.255.255.255
```

```
fw1(config)# show run object-group
object-group network REMOTES
     network-object host 172.30.0.50
     network-object host 172.30.0.51
object-group network DMZ1
     network-object host 192.168.1.10
     network-object host 192.168.1.12
object-group network DMZ2
     network-object host 192.168.2.10
object-group network ALL_DMZ
     group-object DMZ1
     group-object DMZ2
 object-group service BASIC
     port-object eq http
     port-object eq smtp
```
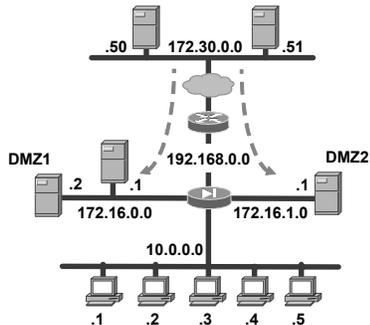
```
fw1(config)# access-list aclout permit tcp
   object-group REMOTES object-group
   ALL_DMZ object-group BASIC
```

SNPA v4.0—6-19

In the figure, object groups are configured so that one ACL entry enables remote hosts 172.30.0.50 and 172.30.0.51 to initiate HTTP and Simple Mail Transfer Protocol (SMTP) connections to DMZ1 and DMZ2 hosts in the ALL_DMZ nested group. With object grouping, one ACL entry is required. Without object grouping, the following ACL entries would be required:

```
access-list outside permit tcp host 172.30.0.50 host
192.168.1.10 eq http
access-list outside permit tcp host 172.30.0.50 host
192.168.1.10 eq smtp
access-list outside permit tcp host 172.30.0.51 host
192.168.1.10 eq http
access-list outside permit tcp host 172.30.0.51 host
192.168.1.10 eq smtp
access-list outside permit tcp host 172.30.0.50 host
192.168.1.12 eq http
access-list outside permit tcp host 172.30.0.50 host
192.168.1.12 eq smtp
access-list outside permit tcp host 172.30.0.51 host
192.168.1.12 eq http
access-list outside permit tcp host 172.30.0.51 host
192.168.1.12 eq smtp
access-list outside permit tcp host 172.30.0.50 host
192.168.2.10 eq http
access-list outside permit tcp host 172.30.0.50 host
192.168.2.10 eq smtp
access-list outside permit tcp host 172.30.0.51 host
192.168.2.10 eq http
access-list outside permit tcp host 172.30.0.51 host
192.168.2.10 eq smtp
```

Displaying Configured Object Groups

firewall(config)#

```
show running-config [all] object-group [protocol |
   service | network | icmp-type | id obj_grp_id]
```

• **Displays object groups in the configuration**

```
fw1# show run object-group
object-group network DMZ1
  network-object host 192.168.1.10
  network-object host 192.168.1.12
object-group network DMZ2
  network-object host 192.168.2.10
object-group network ALL_DMZ
  group-object DMZ1
  group-object DMZ2
```

SNPA v4.0—6-20

Use the **show running-config object-group** command to display a list of the currently configured object groups. The security appliance displays defined object groups by their group identifier when the **show running-config object-group id** *grp_id* command form is entered and by group type when the **show running-config object-group** command is entered with the **protocol**, **service**, **icmp-type**, or **network** option. When you enter **show running-config object-group** without a parameter, all defined object groups are shown.

The syntax for the **show running-config object-group** command is as follows:

```
show running-config [all] object-group [protocol | service |
network | icmp-type | id obj_grp_id]
```

icmp-type	(Optional) Displays ICMP-type object groups.
id *obj_grp_id*	(Optional) Displays the specified object group.
network	(Optional) Displays network object groups.
protocol	(Optional) Displays protocol object groups.
service	(Optional) Displays service object groups.

Removing Configured Object Groups

firewall(config)#

```
no object-group service obj_grp_id {tcp | udp | tcp-
    udp}
```

- **Removes a specific service object group**

firewall(config)#

```
no object-group protocol | network | icmp-type
    obj_grp_id
```

- **Removes a specific protocol, network, or ICMP-type object group**

firewall(config)#

```
clear configure object-group [{protocol | service |
    icmp-type | network}]
```

- **Removes all object groups or all object groups of a specific type**

```
fw1(config)# no object-group network ALL_DMZ
fw1(config)# clear config object-group protocol
```

Any **object-group** command can be removed with its **no** form. Use the **no object-group** command to remove a specific object group.

The syntax for the **no object-group** commands is as follows:

```
no object-group {protocol | network | icmp-type} obj_grp_id
no object-group service obj_grp_id {tcp | udp | tcp-udp}
```

icmp-type	Defines a group of ICMP types, such as echo and echo-reply. After entering the main **object-group icmp-type** command, add ICMP objects to the ICMP-type group with the **icmp-object** and the **group-object** commands.
network	Defines a group of hosts or subnet IP addresses. After entering the main **object-group network** command, add network objects to the network group with the **network-object** and the **group-object** commands.
obj_grp_id	Identifies the object group (one to 64 characters) and can be any combination of letters, digits, and the characters "_", "-", and ".".
protocol	Defines a group of protocols, such as TCP and UDP. After entering the main **object-group protocol** command, add protocol objects to the protocol group with the **protocol-object** and the **group-object** commands.
service	Defines a group of TCP and UDP port specifications, such as "eq smtp" and "range 2000 2010." After entering the main **object-group service** command, add port objects to the service group with the **port-object** and the **group-object** commands.
tcp	Specifies that the service group is used for TCP.
tcp-udp	Specifies that the service group can be used for TCP and UDP.
udp	Specifies that the service group is used for UDP.

The **clear configure object-group** command can be used to remove all object groups or all object groups of a specific type. When entered without a parameter, the **clear configure object-group** command removes all defined object groups that are not being used in a command. Using the **protocol**, **service**, **icmp-type**, or **network** parameter removes all defined object groups that are not being used in a command for that group type only. An object group cannot be removed if it is part of an active ACL and its removal would result in the ACL becoming incomplete or invalid.

The syntax for the **clear configure object-group** command is as follows:

```
clear configure object-group [{protocol | service | icmp-type
| network}]
```

icmp-type	(Optional) Clears all ICMP-type groups.
network	(Optional) Clears all network groups.
protocol	(Optional) Clears all protocol groups.
service	(Optional) Clears all service groups.

Summary

This topic summarizes what you have learned in this lesson.

Summary

- **You can group network objects, services, protocols, and ICMP message types to reduce the number of ACEs required to implement your security policy.**

- **The main object grouping command, the** object-group **command, names your object group and enables a subcommand mode for the type of object you specify.**

- **Members of an object group are defined in its subcommand mode.**

- **Hierarchical, or nested, object grouping enables greater flexibility and modularity for specifying entries within ACLs.**

SNPA v4.0—6-22

Authentication, Authorization, and Accounting

Overview

This lesson introduces security appliance authentication, authorization, and accounting (AAA). Then the lesson discusses how to configure each component—authentication, authorization, and accounting—on a Cisco security appliance.

Objectives

Upon completing this lesson, you will be able to define, configure, and monitor AAA in Cisco security appliances. This includes being able to meet these objectives:

- Define and compare authentication, authorization, and accounting

- Install and configure Cisco Secure ACS

- Describe the differences between authentication, authorization, and accounting

- Define and configure security appliance access authentication

- Define and configure cut-through proxy authentication

- Define and configure tunnel access authentication

- Define and configure user authorization

- Define and configure downloadable ACLs

- Define and configure accounting

Introduction to AAA

This topic introduces the concepts of AAA and how Cisco security appliances support them.

Authentication, Authorization, and Accounting

Cisco.com

Web server

Cisco Secure ACS server

Internet

- Authentication
  - Who you are
- Authorization
  - What you can do
- Accounting
  - What you did

© 2005 Cisco Systems, Inc. All rights reserved.   SNPA v4.0—7-4
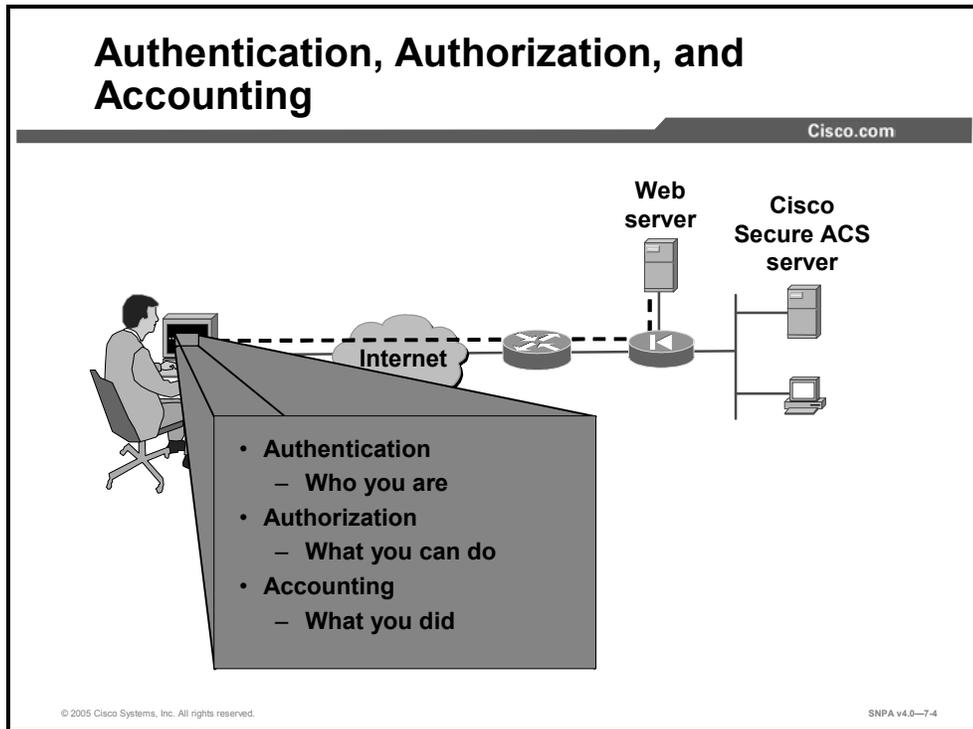
AAA is used to tell the security appliance who the user is, what the user can do, and what the user did. Authentication is valid without authorization. Authorization is never valid without authentication.

Suppose you have 100 users and you want only six of these users to be able to use FTP, Telnet, HTTP, or HTTPS from outside the network. Configure the security appliance to authenticate inbound traffic and give each of the six users an identification on the AAA server. With simple authentication, these six users are authenticated with a username and password, then permitted access to the network. The other 94 users cannot access the network. The security appliance prompts users for their username and password, then passes their username and password to the AAA server. Depending on the response, the security appliance permits or denies the connection.

Suppose one of these users, baduser, is "technically challenged." You want to allow baduser to use HTTP, but not Telnet, to the network. This means you must add authorization, that is, in addition to authenticating who the users are, you must authorize what they can do. When you add authorization to the security appliance, it first sends the technically challenged user's username and password to the AAA server, then sends an authorization request telling the AAA server which command baduser is trying to use. With the server set up properly, baduser is allowed to use HTTP but is not allowed to use Telnet.

Types of Authentication

Cisco.com

Types of authentication:
- **Authenticate access to the security appliance**
- **Authenticate access through the security appliance**
  - **Cut-through proxy**
- **Authentication tunnel access**
  - **IPSec**
  - **SSL VPN**

Security Appliance Console Access

Security Appliance Console Access

Internet

Authentication

Web server

Cut-through Proxy

Internet

Authentication

IPSec/SSL VPN
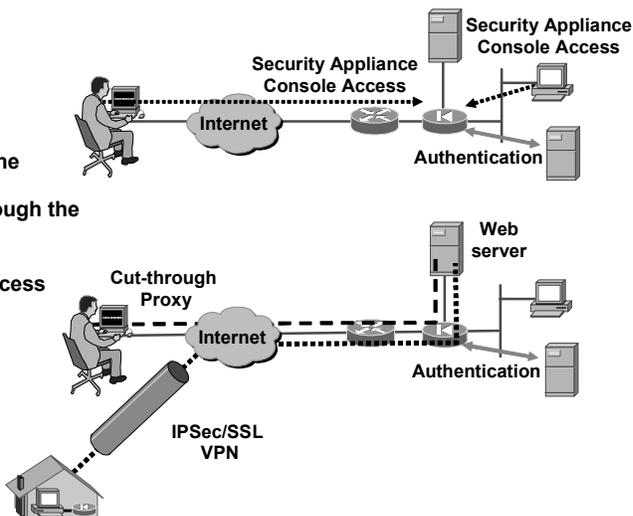
SNPA v4.0—7-5

Three types of authentication are available: security appliance access, cut-through proxy, and tunnel access. Security appliance access enables the administrator to require authentication verification to access the security appliance. The access authentication service options available are as follows: **enable**, **serial**, **ssh**, **http**, and **telnet**. In the example in the figure, a remote administrator is attempting to access the security appliance via Secure Shell (SSH) Protocol from the user's home office while a local administrator is attempting to access the security appliance via Telnet. Both must be authenticated before they are permitted to access the security appliance.

For cut-through proxy authentication, the security appliance can be configured to require user authentication for a session through the security appliance, as specified in the **aaa authentication** command. Only Telnet, FTP, HTTP, and HTTPS sessions can be intercepted to authenticate users. In the example in the figure, a remote user is attempting an HTTP session with the web server. If the user is authenticated by the security appliance, the HTTP session to the web server is connected, cut-through. The security appliance then shifts the session flow and all traffic flows directly between the server and the client while maintaining session state information.

For tunnel access authentication, the security appliance can be configured to require a remote tunnel user to authenticate before full tunnel establishment. In the example in the figure, a remote user establishes an IPSec tunnel with the corporate office to gain access to the corporate web server. Before the tunnel is fully established, the security appliance will prompt the remote user for a username and password. The credentials are verified before the remote user's tunnel is fully established and they are allowed to access the corporate web server.

Types of Authorization

Cisco.com

Types of authorization:

- Console access—specifies whether command execution is subject to authorization.
- Cut-through proxy— specifies what "through" services are subject to authorization.
- Tunnel access-- specifies what "tunnel" services are authorized.

Security Appliance Console Access

Security Appliance Console Access

Authorization

Internet

Web server

Cut-through Proxy

Internet

Authorization

IPSec/SSL VPN
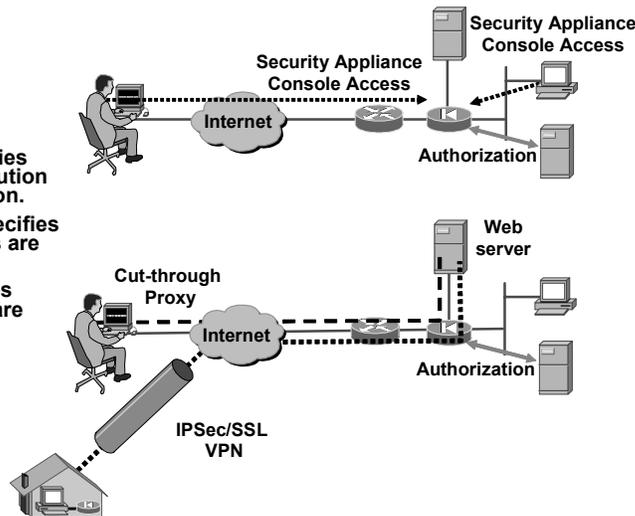
SNPA v4.0—7-6

Three types of authorization are available: security appliance access, cut-through proxy, and tunnel access. Security appliance access authorization is a way of facilitating and controlling administration, including who can access the security appliance and which commands they can execute. The administrator assigns commands to a privilege level. The administrator creates user accounts and links a privilege level to each user. When a console user attempts to access the security appliance console, they are prompted for a username and password. When authenticated, the console user is granted the access level privileges assigned to their user account.

If the administrator wants to allow all authenticated users to perform all HTTP, HTTPS, FTP, and Telnet operations through the security appliance, authentication is sufficient and authorization is not needed. But if there is reason to allow only some subset of users, or to limit users to certain sites and protocols, authorization is needed. The security appliance supports two basic methods of user authorization of cut-through proxy:

- The security appliance is configured with rules specifying which connections need to be authorized by the AAA server. When the first packet of a traffic flow matches a predefined rule, the AAA server is consulted by the security appliance for access rights. The AAA server returns a permit or deny authorization message.

- The security appliance is configured with rules that specify which connections need to be authenticated by the AAA server. The AAA server is configured with authorization rules that are assigned to the authenticating user. The authorization rules come in the form of access control lists (ACLs). An ACL is attached to the user or group profile on the AAA server. When the first packet of a traffic flow matches a predefined rule, the AAA server is consulted by the security appliance for access rights, permit or deny. During the authentication process, if the end user is authenticated, the Cisco Secure Access Control Server (Cisco Secure ACS) downloads an ACL to the security appliance. The ACL is applied to the traffic flow. The Cisco Secure ACS has the ability to store ACLs and download them to the security appliance.

When remote users attempt to establish a tunnel to the security appliance, the administrator can force the tunnel users to authenticate before granting them access to the security appliance. When a tunnel user authenticates, the security appliance retrieves tunnel information for the defined user or group. The tunnel authorization information can include such information as virtual private network (VPN) access hours, simultaneous logins, client block rules, personal computer firewall type, idle timeout, and so on. The tunnel group information is applied to the tunnel before the tunnel is fully established.

Types of Accounting

Security Appliance Console Access

Security Appliance Console Access

Types of accounting:
- **Accounting of security appliance console access**
- **Accounting of access through the security appliance**
  - **Cut-through proxy**
- **Accounting of tunnel connections**
  - **IPSec**
  - **SSL VPN**

Accounting

Web server

Cut-through Proxy

Internet

Accounting

IPSec/SSL VPN
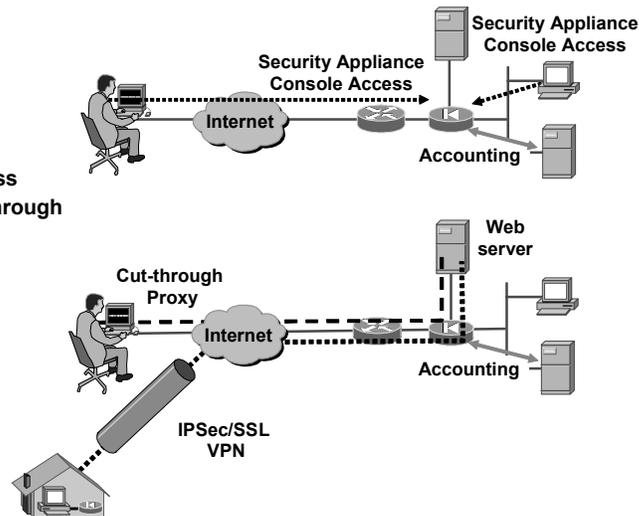
SNPA v4.0—7-7

An administrator can configure the security appliance to enable accounting for specific network services. Accounting records are generated to track the initiation and termination of predefined sessions. The security appliance can be configured to generate accounting records for configuration changes. For example, accounting records can track when a Telnet user logged in to the security appliance, at what privilege level, what configuration commands were entered, and when the session was terminated. It can track the beginning and end of a web session between a remote user and the corporate DMZ web server. It can also be used to track remote tunnel access, when it started and finished. These records are kept on the designated AAA server or servers.

Installation of Cisco Secure ACS for Windows 2000

This topic explains how to install Cisco Secure ACS for Windows 2000.

SNPA v4.0—7-9
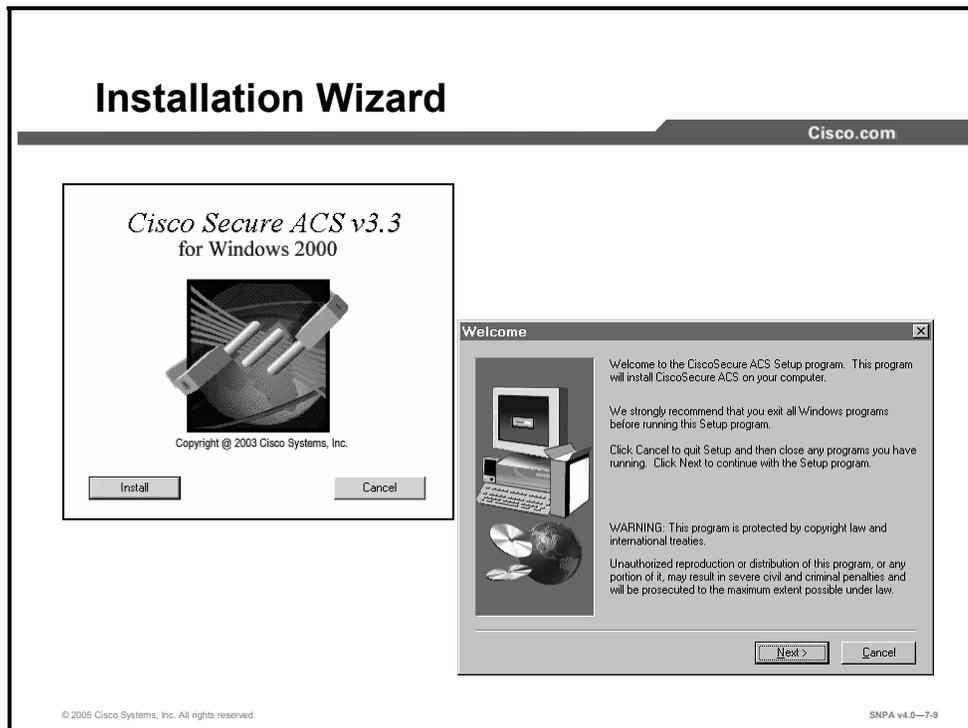
Note	Close all Windows programs before you run the setup program. (Optional) If Cisco Secure ACS is already installed, the Previous Installation window opens. You are prompted to remove the previous version and save the existing database information. Click **Yes, keep existing database** and click **Next** to keep the existing data. To use a new database, deselect the check box and click **Next**. If you selected the check box, the setup program backs up the existing database information and removes the old files.

Complete the following steps to start installation of Cisco Secure ACS for Windows 2000:

Step 15   To install Cisco Secure ACS on your student PC from the files on your hard drive, open the Cisco Secure ACS v3.3.X folder on your desktop and double-click **setup.exe**.

Step 16   Click **Accept** to accept the Software License Agreement. The Welcome window opens.

Step 17   Read the Welcome window. Click **Next** to continue. The Before You Begin window opens.

Step 18   Read and then select all four check boxes for the items in the Before You Begin frame. This is a reminder of things you should do prior to installation. Click **Next** to continue. The Choose Destination Location window opens.

Step 19   Use the default installation folder indicated in the Choose Destination Location windows by clicking **Next** to continue. The Authentication Database Configuration windows open.

Step 20   Verify that **Check the Cisco Secure ACS database only** is already selected in the Authentication Database Configuration frame. Click **Next** to start the file installation process.

Step 21   Select all six items displayed in the Advanced Options frame. Click **Next** to continue.

Step 22   Verify that **Enable Log-in Monitoring** is already selected in the Active Service Monitoring frame. Click **Next** to continue.

Step 23   Verify that the following selections in the Cisco Secure ACS Service Initiation window:

- Select Yes, I want to start the Cisco Secure ACS Service now.
- Select Yes, I want Setup to launch the Cisco Secure ACS Administrator from my browser following installation.
- Deselect Yes, I want to review the Readme file.

Step 24   Click **Next** to start the Cisco Secure ACS service.

Step 25   Read the Setup Complete window, then click **Finish** to end the installation wizard and start your web browser with Cisco Secure ACS.

ACS Network Configuration

Cisco.com

© 2005 Cisco Systems, Inc. All rights reserved.   SNPA v4.0—7-10
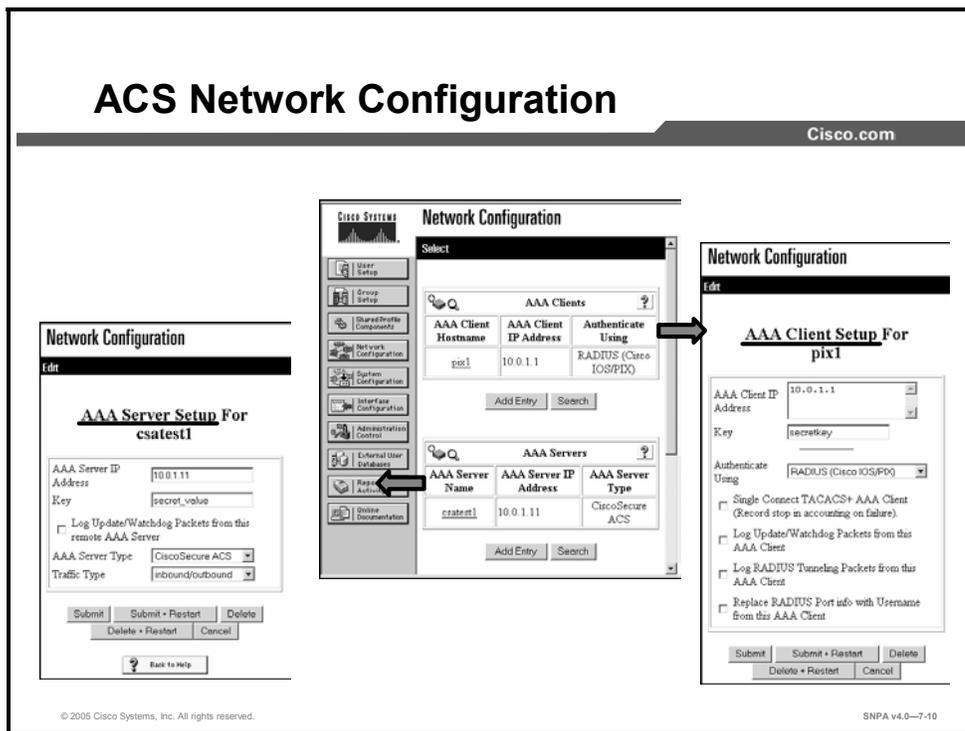
For the Cisco Secure ACS to communicate with the security appliance, the administrator must configure the AAA client and AAA server information. The AAA client is the security appliance. The AAA server is the Cisco Secure ACS information. Complete the following steps to add the security appliance to the Cisco Secure ACS AAA client database in your Windows 2000 server:

Step 26   The Cisco Secure ACS interface should now be displayed in your web browser. Click **Network Configuration** to open the Network Configuration window.

Step 27   Under AAA Client group box, click **Add Entry**.

Step 28   In the AAA Client Hostname field, enter **pixP**, the hostname of the security appliance.

Step 29   In the AAA Client IP Address field, enter **10.0.P.1**, the IP address of the security appliance inside interface.

Step 30   In the Key field, enter **secretkey**.

Step 31   In the Authentication Using drop-down menu, select **RADIUS (Cisco IOS/PIX)** for RADIUS protocol applications. Select **TACACS+ (Cisco IOS/PIX)** for Terminal Access Controller Access Control System Plus (TACACS+) protocol applications.

Step 32   Click **Submit + Restart** to submit the changes.

Security Appliance Access Authentication Configuration

This topic discusses how to configure authentication on Cisco security appliances.

Types of Security Appliance Access Authentication

Cisco.com

Security Appliance console access

Security Appliance console access

Internet

Local, RADIUS, or TACACS+

Authentication Server

Authentication
   Who you are
Authorization
   What you can do
Accounting
   What you did

Types of security appliance console authentication
- **Telnet**   - **Serial**
- **SSH**   - **Enable**

SNPA v4.0—7-12
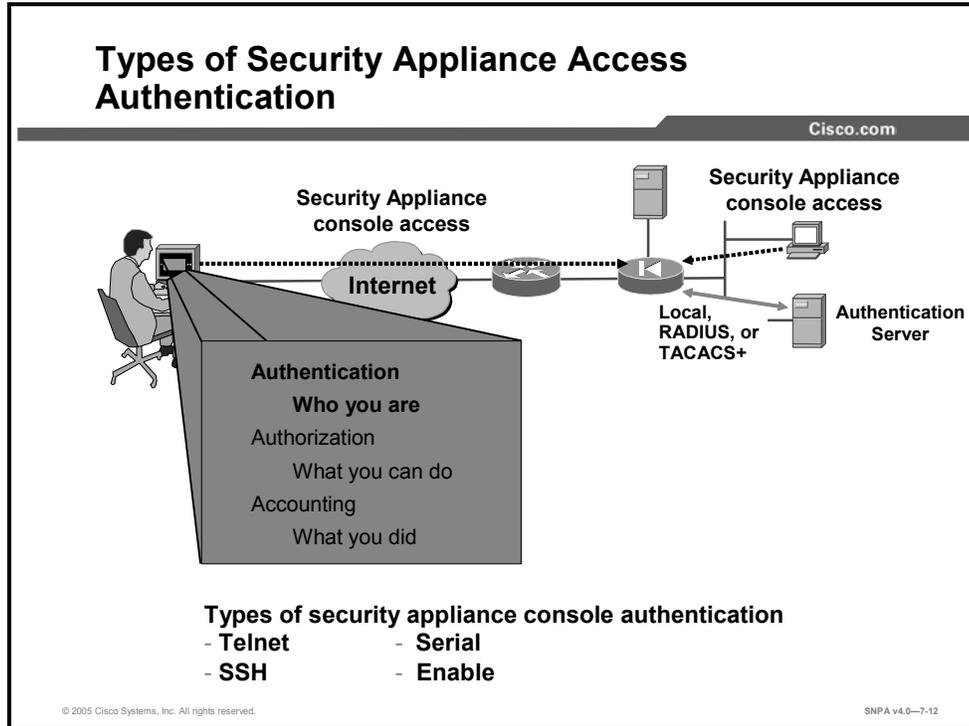
The **aaa authentication serial console** command enables you to require authentication verification to access the console of the security appliance unit. Authenticated access to the security appliance console involves different types of prompts, depending on the option you choose with the **aaa authentication** [**serial** | **enable** | **telnet** | **ssh**] **console** command. The **enable** and **ssh** options allow three tries before stopping access attempts with an "access denied" message. By default, both the **serial** and **telnet** options cause the user to be prompted continually until that user successfully logs in. The administrator may choose to configure a maximum failed attempts value for local database users. The **serial** option requests a username and password before the first command-line prompt on the serial console connection. The **telnet** option forces you to specify a username and password before the first command-line prompt of a Telnet console connection. The **enable** option requests a username and password before accessing privileged mode for serial, Telnet, or SSH connections. The **ssh** option requests a username and password before the first command-line prompt on the SSH console connection.

Telnet access to the security appliance console is available from any internal interface and from the outside interface within an IPSec tunnel. SSH access to the security appliance console is available from any interface without IPSec configured and requires the previous configuration of the **ssh** command.

Security Appliance Access Authentication: Configuration Steps

Access authentication configuration steps:

- **Specify an AAA server group.**

```
fw1(config)# aaa-server <server-tag> protocol <protocol>
```

- **Designate an authentication server.**

```
fw1(config)# aaa-server <server-tag> <(if_name)> host
<ip_address>
```

- **Enable security appliance access authentication.**

```
fw1(config)# aaa authentication [serial | enable |
  telnet | ssh | http] console server_tag [LOCAL]
```

SNPA v4.0—7-13

Configuring interactive user authentication is a three-step process, as follows:

Step 33 Specify an AAA server group. The administrator defines a group name and the authentication protocol.

Step 34 Designate an authentication server. The administrator defines the location of the AAA server and defines a key.

Step 35 Enable user authentication. The administrator defines a rule to specify which security appliance access method to authenticate and which authentication server to reference.

Specify an AAA Server Group

Cisco.com

Web server

Internet

NY_ACS server
10.0.0.2
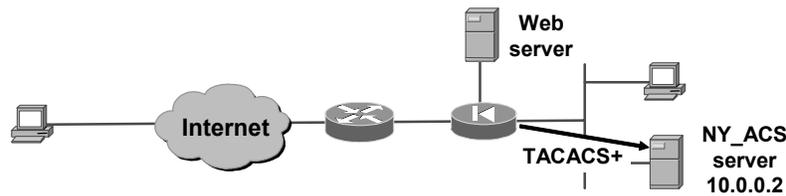
TACACS+

firewall (config)#

```
aaa-server <server-tag> protocol <protocol>
```

- **Assign TACACS+ or RADIUS protocol to a server tag.**

```
fw1(config)# aaa-server NY_ACS protocol tacacs+
```

SNPA v4.0—9-27

Use the **aaa-server** command to specify AAA server groups. For security appliance access authentication, the security appliance supports TACACS+, RADIUS and local database authentication. The security appliance enables you to define separate groups of TACACS+ or RADIUS servers for specifying different types of traffic, such as a TACACS+ server for inbound traffic and another for outbound traffic. The **aaa** command references the server tag to direct authentication, authorization, or accounting traffic to the appropriate AAA server.

You can have up to 15 single-mode server groups, and each group can have up to 16 AAA servers, for a total of up to 240 TACACS+ or RADIUS servers. (Or, the security appliance supports seven multimode server groups, and each group can have up to four AAA servers.) When a user logs in, the servers are accessed one at a time, starting with the first server in the server group configuration, until a server responds.

Note	If you are upgrading your security appliance and have **aaa** command statements in your configuration, using the default server groups enables you to maintain backward compatibility with the **aaa** command statements in your configuration.

Note	The previous **server type** option at the end of the **aaa authentication** and **aaa accounting** commands has been replaced with **aaa-server** *server tag*. Backward compatibility with previous versions is maintained by the inclusion of two default protocols for TACACS+ and RADIUS.

The syntax for the **aaa-server** commands is as follows:

```
aaa-server server_tag protocol protocol
```

clear config aaa-server [*<tag>* *[host<hostname>]*]

server_tag	An alphanumeric string that is the name of the server group. Use the server group name in the **aaa** command to associate **aaa authentication**, **aaa authorization**, and **aaa accounting** command statements with an AAA server.
protocol	The AAA protocol that the servers in the group support: Kerberos, Lightweight Directory Access Protocol (LDAP), Windows NT, RADIUS, SecurID, and TACACS+.

AAA Server Group—Sub-Command
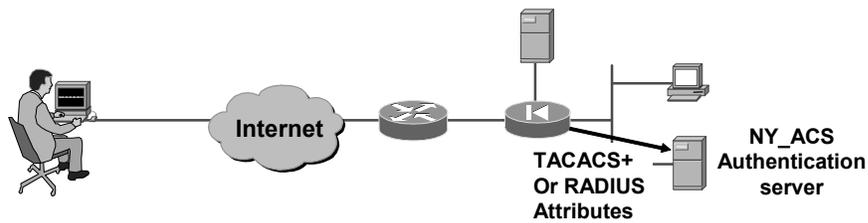
- **Assign TACACS+ or RADIUS server group attributes.**

```
fw1(config-aaa-server)# ?

aaa-server group configuration commands:
  accounting-mode      Enter this keyword to specify accounting mode
  max-failed-attempts  Specify the maximum number of failures that will be
                       allowed for any server in the group before that server
                       is deactivated
  no                   Remove an item from aaa-server group configuration
  reactivation-mode    Specify the method by which failed servers are
                       reactivated
```

SNPA v4.0—7-15

For any RADIUS or TACACS+ server group, an administrator can also set the accounting mode, the maximum allowed failed attempts, and the reactivation method for a group of servers. The configuration options for the **aaa-server** subcommand are as follows:

- **accounting-mode**—Enter this keyword to specify the accounting mode. It indicates whether accounting messages are sent to a single server (single mode) or to all servers in the group (simultaneous mode).

- **max-failed-attempts**—Specify the maximum number of failures that will be allowed for any server in the group before that server is deactivated.

- **reactivation-mode**—Specify the method by which failed servers are reactivated. The administrator can choose to reactivate failed servers after a configurable number of minutes of down time or wait until all other servers in this group are inactive.

Designate an Authentication Server
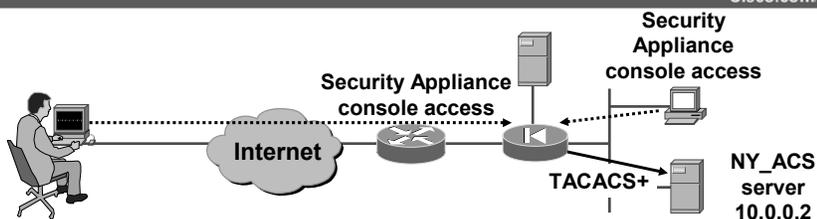
firewall (config)#

```
aaa-server server_tag (if_name) host ip_address
```

- **Identifies the AAA server for a given server tag.**
- **Configures aaa-server sub-commands**

```
fw1(config)# aaa-server NY_ACS (inside) host 10.0.0.2
fw1(config-aaa-server)# key secretkey
fw1(config-aaa-server)# timeout 10
```

SNPA v4.0—7-16

The next step is to define the AAA server and the AAA server attributes. The administrator defines the AAA server using the following parameters:

- *server_tag*: Name of the server group. There can be up to 15 single-mode groups or four multimode groups.

- *if_name*: Name of the interface on which the AAA server resides.

- *ip-address*: IP address of the AAA server.

The administrator defines the subcommand attributes for the AAA server. The subcommand attributes vary according to the AAA protocol supported by the server. The following are attributes supported by a RADIUS AAA server group:

- *key*: The key that is used to encrypt data between the security appliance and the AAA server. The key between the security appliance and the AAA server must match.

- **accounting-port**: Specifies the port number to be used for RADIUS accounting

- **authentication-port**: Specifies the port number to be used for RADIUS authentication

- **radius-common-pw**: Specifies a common password for all RADIUS authorization transactions

- **retry-interval**: Specifies the amount of time between retry attempts for a RADIUS server.

- **timeout** *seconds*: Specifies the maximum time to wait for response from configured server.

In the example in the figure, there is an AAA server that belongs to the NY_ACS group. It is located on the inside interface and has an IP address of 10.0.0.2. The encryption key is "secretkey," and the request timeout is 10 seconds.

The syntax for the **aaa-server** commands is as follows:

```
aaa-server server_tag (if_name) host ip_address key timeout seconds
```

server_tag	A case-sensitive alphanumeric string that is the name of the server group. Use the server group name in the **aaa** command to associate **aaa authentication**, **aaa authorization**, and **aaa accounting** command statements with an AAA server.
if_name	The interface name on the side where the AAA server resides.
host *ip_address*	The IP address of the TACACS+ or RADIUS server.
key	A case-sensitive, alphanumeric keyword of up to 127 characters that is the same value as the key on the AAA server. Any characters entered past the limit of 127 are ignored. The key is used for encrypting data between the client and the server. The key must be the same on the client and server systems. Spaces are not permitted in the key, but other special characters are allowed. If a key is not specified, encryption does not occur.
timeout *seconds*	A retransmit timer that specifies the duration of the period during which the security appliance retries access. The security appliance retries access to the AAA server four times, each time for the length of this period, before choosing the next AAA server. The default is 10 seconds. The maximum time is 300 seconds. For example, if the timeout value is 10 seconds, the security appliance retransmits for 10 seconds, and if no acknowledgment is received, tries three times more, for a total of 40 seconds, to retransmit data before the next AAA server is selected.

Authentication of Console Access
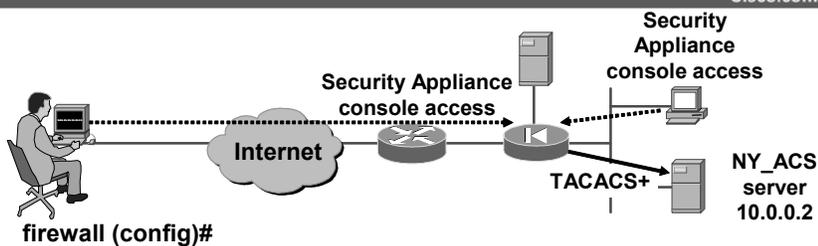
```
firewall (config)#

aaa authentication {serial | enable | telnet | ssh |
  http} console server_tag [LOCAL]
```

- Defines a console access method that requires authentication.
- Identifies the authentication server_tag—authentication server or LOCAL.
- Enables fallback to LOCAL security appliance database.

```
fw1(config)# aaa authentication serial console NY_ACS LOCAL
fw1(config)# aaa authentication enable console NY_ACS LOCAL
fw1(config)# aaa authentication telnet console NY_ACS LOCAL
fw1(config)# aaa authentication ssh console NY_ACS LOCAL
```

SNPA v4.0—7-17

Use the **aaa authentication console** command to require authentication verification to access the security appliance's console.

Authenticated access to the security appliance console involves different types of prompts, depending on the option you choose with the **aaa authentication console** command:

- **enable**: Allows three tries before stopping access attempts with an "access denied" message. The **enable** option requests a username and password before accessing privileged mode for serial, Telnet, or SSH connections.

- **serial**: Causes the user to be prompted continually by default until that user successfully logs in. (A limit can be set by the administrator with the **aaa local authentication attempts max-fail** command.) The **serial** option requests a username and password before the first command-line prompt on the serial console connection.

- **ssh**: Allows three tries before stopping access attempts with a "rejected by server" message. The **ssh** option requests a username and password before the first command-line prompt appears.

- **telnet**: Causes the user to be prompted continually by default until that user successfully logs in. (A limit can be set by the administrator with the **aaa local authentication attempts max-fail** command.) The **telnet** option requests a username and password before the first command-line prompt of a Telnet console connection. You can enable Telnet to the security appliance on all interfaces. The security appliance enforces that all Telnet traffic to the outside interface is protected by an IPSec tunnel. To enable a Telnet session to the outside interface, configure IPSec and enable Telnet on the outside interface.

The syntax for the **aaa authentication console** commands is as follows:

```
aaa authentication {serial | enable | telnet | ssh | http} console
server_tag [LOCAL]
```

serial	Verifies access for the security appliance's serial console.
enable	Verifies access for the security appliance's privilege mode.
telnet	Verifies Telnet access to the security appliance console.
ssh	Verifies SSH access to the security appliance console.
http	Verifies HTTP access to the security appliance (via Cisco PIX Device Manager [PDM]).
console	Specifies that access to the security appliance console requires authentication.
server_tag	The server tag that is set with the **aaa-server** command. To use the local security appliance user authentication database, enter **LOCAL** for this parameter.

To configure administrative authentication to support fallback to the local user database if all servers in the specified server group or groups are disabled, use the **aaa authentication** command with the **LOCAL** option specified. This feature is disabled by default. In the example in the figure, notice that each security appliance access method authenticates using the NY_ACS server. In the event that the NY_ACS server is no longer accessible, the security appliance is configured to access the local database for console access authentication.

How to Add Users to Cisco Secure ACS
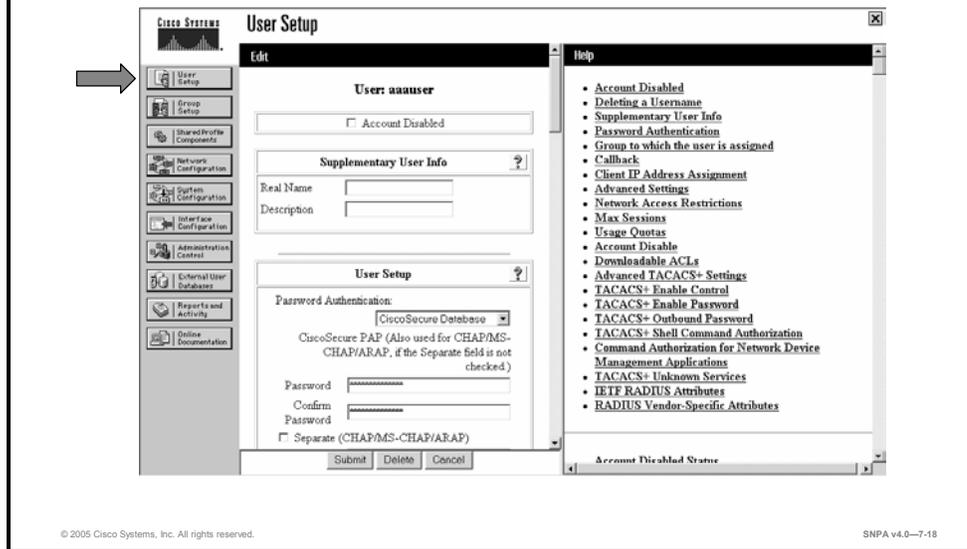
After the AAA server and AAA authentication console are configured, the administrator can add users to the AAA server and the local database on the security appliance. To add users to the Cisco Secure ACS, complete the following steps:

Step 36   Click User Setup from the navigation bar. The Select window opens.

Step 37   Enter a name in the User field.

Note   The username can contain up to 32 characters. Names cannot contain the following special characters: #, ?, ", *, >, and <. Leading and trailing spaces are not allowed.

Step 38   Click Add/Edit. The Edit window opens. The username being added or edited appears at the top of the window.

The Edit window contains the following sections:

■   Account Disabled

■   Supplementary User Info

■   User Setup

■   Account Disable

Account Disabled

If you need to disable an account, select the Account Disabled check box in the Account Disabled section to deny access for this user.

Note   You must click **Submit** to have this action take effect.

Supplementary User Info

In this section, you can enter supplemental information to appear in each user profile. The fields shown in the following list are available by default. You can insert additional fields—

click **Interface Configuration** in the navigation bar, then click **User Data Configuration** (configuring supplemental information is optional):

■ Real Name: If the username is not the user's real name, enter the real name here.

■ Description: Enter a detailed description of the user.

User Setup

In the User Setup group box, you can edit or enter the following information for the user as applicable:

■ Password Authentication: From the drop-down menu, choose a database to use for username and password authentication. You can select the Windows Database or the CiscoSecure Database. The Windows Database option authenticates a user with an existing account in the Windows User Database located on the same machine as the Cisco Secure ACS. The CiscoSecure Database option authenticates a user from the local Cisco Secure ACS database. If you select this database, enter and confirm the Password Authentication Protocol (PAP) password to be used. The Separate (CHAP/MS-CHAP/ARAP) option is not used with the security appliances.

Note   The Password and Confirm Password fields are required for all authentication methods except for all third-party user databases.

■ Group to which the user is assigned: From the Group to which the user is assigned drop-down menu, choose the group to assign the user to. The user inherits the attributes and operations assigned to the group. By default, users are assigned to the Default Group. Users who authenticate via the Unknown User method and who are not found in an existing group are also assigned to the Default Group.

■ Callback: This information is not used with the security appliances.

■ Client IP Address Assignment: This information is not used with security appliances.

Account Disable

The Account Disable group box can be used to define the circumstances under which the user's account will become disabled.

Note   This action is not to be confused with account expiration resulting from password aging. Password aging is defined for groups only, not for individual users.

■ Never: Select this button to keep the user's account always enabled. This is the default.

■ Disable account: Select this button to disable the account under the circumstances you specify in the following fields:

— Date exceeds: From the drop-down menu, choose the month, date, and year on which to disable the account. The default is 30 days after the user is added.

— Failed attempts exceed: Select the check box and enter the number of consecutive unsuccessful login attempts to allow before disabling the account. The default is 5.

■ Failed attempts since last successful login: This counter shows the number of unsuccessful login attempts since the last time this user logged in successfully.

■ Reset current failed attempts count on submit: If an account is disabled because the failed attempts count has been exceeded, select this check box and click **Submit** to reset the failed attempts counter to 0 and reinstate the account.

If you are using the Windows Database, this expiration information is in addition to the information in the Windows user account. Changes here do not alter settings configured in Windows.

Step 39   When you have finished configuring all user information, click **Submit**.

How to Add Users to the LOCAL Database

Cisco.com

Telnet

Internet

Authentication via LOCAL database
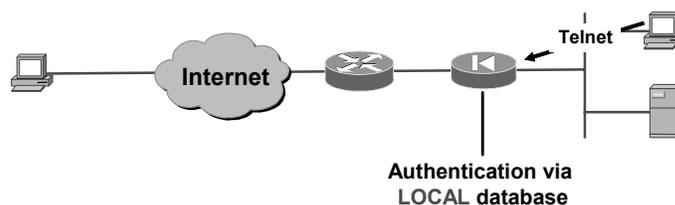
firewall (config)#

```
username {name} {nopassword | password password}
```

- **Specify an** username **in the LOCAL database.**
- **Specify the** LOCAL **keyword in the authentication command.**
- **(Optional) Specify the maximum number of failed attempts after which a user is locked out**

```
fw1(config)# username admin1 password cisco123
fw1(config)# aaa authentication telnet console LOCAL
```

SNPA v4.0—7-19

An administrator can configure a local database in the security appliance. When authenticating console access, the local database can be the primary means of authenticating console access or can serve as a fallback database when the AAA server is no longer accessible. Use the **username** command to create user accounts in the local user database. You can create a password for the user or you can use the **nopassword** keyword to create a user account with no password. Use the **encrypted** keyword if the password you are supplying is already encrypted, and use **privilege** *level* to assign a privilege level to the user. In the example in the figure, the administrator defines a user, with the username admin1 and a password of cisco123, in the local database of the security appliance. When someone attempts a Telnet access to the security appliance, the user is authenticated with the local internal database of the security database.

To delete an existing user account, use the **no username** command. To remove all the entries from the user database, enter the **clear config username** command.

The syntax for the **username** commands is as follows:

```
username username nopassword | password password [encrypted]
[privilege level]
```

username	The username that is assigned to the user account.
nopassword	Used to create a user account with no password.
password	The password that is assigned to the user account.
encrypted	Specifies that the password you are supplying is already encrypted.
level	Specifies the privilege level for the user account.

Maximum Failed Attempts

Cisco.com

Telnet

Internet

Authentication via
LOCAL database
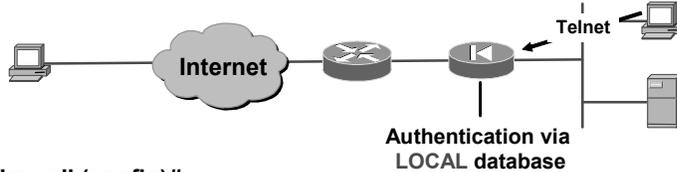
firewall (config)#

```
aaa local authentication attempts max-fail <fail-attempts>
```

- **Specify the maximum number of failed attempts after which a user is locked out**

```
clear aaa local user {fail-attempts | lockout} {all | username
  <name>}
```

- **Clear lockout condition, or the number of failed attempts, for a user, or all users.**

```
fw1(config)# aaa local authentication attempts max-fail 3
fw1 # show aaa local user
Lock-time  Failed-attempts  Locked  User
15:34:56            3        Y      admin1
```

Authenticated access to the security appliance console involves different types of prompts, depending on the option you choose with the **aaa authentication console** command:

- **enable**: Allows three tries before stopping access attempts with an "access denied" message.

- **serial**: Causes the user to be prompted *continually by default* until that user successfully logs in.

- **ssh**: Allows three tries before stopping access attempts with a "rejected by server" message.

- **telnet**: Causes the user to be prompted *continually by default* until that user successfully logs in.

The **aaa local authentication attempts max-fail <fail-attempts>** command enables the administrator to set a limit on the number of retries for serial and Telnet access users. In the example in the figure, admin1 attempts to gain console access to the security appliance. After three failed attempts, admin1 is locked out. The administrator can use the **show aaa local user** command to view the local user lock-time, failed-attempts, and locked status. To clear the failed-attempts counter or lockout status by user or for all users, the administrator can use the **clear aaa local user {fail-attempts | lockout} {all | username <name>}** command.

Show LOCAL Users

Telnet — "admin1"

Authentication via
LOCAL
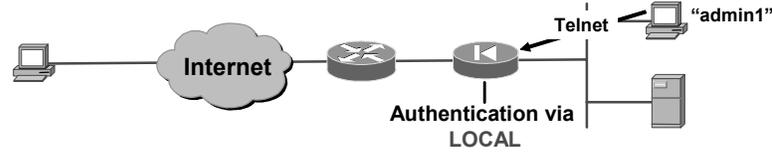
```
fw1(config)# aaa authentication telnet console LOCAL
fw1 # show aaa local user
Lock-time  Failed-attempts  Locked  User
     -              2          N      admin1

fw1 # show aaa-server LOCAL
Server Group:    LOCAL
Server Protocol: Local database
Server Address:  None
Server port:     None
Server status:   ACTIVE, Last transaction at 15:38:37 UTC Wed Dec 1 2004
Number of pending requests           0
Average round trip time              0ms
Number of authentication requests    1
Number of authorization requests     0
Number of accounting requests        0
Number of retransmissions            0
Number of accepts                    1
```

SNPA v4.0—7-21

The administrator can view the statistics associated with the local users and the local server. With the **show local user** command, the administrator can view the lock-time, failed-attempts and locked status of each user in the local database. With the **show aaa-server LOCAL** command, the administrator can view the status of the local server.

How to Change the Authentication Prompts

Cisco.com

Please Authenticate
Username: asjdkl
Password:
Authentication Failed, Try Again
Please Authenticate to the Firewall
Username: asjfkl
Password:
You've been Authenticated

firewall (config)#

```
auth-prompt [accept | reject | prompt] string
```

- **Defines the prompt users see when authenticating.**
- **Defines the message users get when they successfully or unsuccessfully authenticate.**
- **By default, only username and password prompts are seen.**

```
fw1(config)# auth-prompt prompt Please Authenticate
fw1(config)# auth-prompt reject Authentication Failed, Try Again
fw1(config)# auth-prompt accept You've been Authenticated
```

SNPA v4.0—7-22

Use the **auth-prompt** command to change the AAA challenge text for HTTP, FTP, and Telnet access. This is text that appears above the username and password prompts that you view when logging in.

| Note | Microsoft Internet Explorer displays only up to 37 characters in an authentication prompt; Netscape Navigator displays up to 120 characters; and Telnet and FTP display up to 235 characters in an authentication prompt. |

The syntax for the **auth-prompt** commands is as follows:

```
auth-prompt [accept | reject | prompt] string
```

show run auth-prompt

accept	If a user authentication via Telnet is accepted, the accept message is displayed.
reject	If a user authentication via Telnet is rejected, the reject message is displayed.
prompt	The AAA challenge prompt string follows this keyword. This keyword is optional for backward compatibility.
string	A string of up to 235 alphanumeric characters. Special characters should not be used; however, spaces and punctuation characters are permitted. Entering a question mark or pressing the Enter key ends the string. (The question mark appears in the string.)

How to Change the Authentication Timeouts

- Inactivity timeout
- Absolute timeout

firewall (config)#

```
timeout uauth hh:mm:ss [absolute|inactivity]
```

- **Sets the time interval before users will be required to reauthenticate**
  - **Inactivity: Time interval for inactive sessions (no traffic)**
  - **Absolute: Time interval starts at user login**

```
fw1(config)# timeout uauth 0:30:00 inactivity
fw1(config)# timeout uauth 3:00:00 absolute
```

SNPA v4.0—7-23

Use the **timeout uauth** command to specify how long the cache should be kept after the user connections become idle. The time-out value must be at least 2 minutes. Use the **clear uauth** command to delete all authorization caches for all users, which causes them to reauthenticate the next time they create a connection.

The inactivity and absolute qualifiers cause users to reauthenticate after either a period of inactivity or an absolute duration. The inactivity timer starts after a connection becomes idle. If a user establishes a new connection before the duration of the inactivity timer, the user is not required to reauthenticate. If a user establishes a new connection after the inactivity timer expires, the user must reauthenticate.

The absolute timer runs continuously, but waits and prompts the user again when the user starts a new connection, such as clicking a link after the absolute timer has elapsed. The user is then prompted to reauthenticate. The absolute timer must be shorter than the translation timer, otherwise a user could be prompted again after the session has already ended.

The inactivity timer gives users the best Internet access because they are not regularly prompted to reauthenticate. Absolute timers provide security and manage the security appliance connections better. Being prompted to reauthenticate regularly helps users manage their use of the resources more efficiently. Also, being prompted minimizes the risk that someone will attempt to continue another user's access after the first user leaves the workstation, such as in a college computer lab.

An inactivity timer and an absolute timer can operate at the same time, but you should set the absolute timer duration for a longer period than the inactivity timer. If the absolute timer is set at less than the inactivity timer, the inactivity timer is never invoked. For example, if you set the absolute timer to 10 minutes and the inactivity timer to an hour, the absolute timer prompts the user every 10 minutes, and the inactivity timer will never be started.

If you set the inactivity timer to some duration, but set the absolute timer to 0, users are reauthenticated only after the inactivity time elapses. If you set both timers to 0, users have to reauthenticate on every new connection.

Note   Do not set the time-out duration to 0 seconds when using the virtual HTTP option or passive FTP.

The syntax for the **timeout uauth** commands is as follows:

```
timeout uauth hh:mm:ss [absolute | inactivity]
```

show run timeout

uauth *hh:mm:ss*	Duration before the authentication and authorization cache times out and the user has to reauthenticate the next connection. This duration must be shorter than the translation values. Set to 0 to disable caching.
absolute	Runs the timer continuously, but after timer elapses, waits to reprompt the user until the user starts a new connection (for example, by clicking a link in a web browser). To disable the **absolute** option, set it to 0. The default is 5 minutes.
inactivity	Starts the timer after a connection becomes idle. The default is 0.

Security Appliance Cut-Through Authentication Configuration

This topic discusses how to configure cut-through authentication on Cisco security appliances.

Cut-Through Proxy Operation

Types of cut-through proxy user authentication
- Telnet
- FTP
- HTTP
- HTTPS

Web server

The user makes a request to access the web server.

1

Internet

2 The user is prompted by the Security Appliance.

Username

Enter username for CCO at www.cisco.com:

User Name: Bill Smith
Password: cisco123

OK   Cancel

5 The local username and password are passed to the web server to authenticate.

5

3

Cisco Secure ACS server

4

3 The security appliance queries Cisco Secure ACS for the remote username and password.

4 If Cisco Secure ACS authenticates, the user is "cut through" the security appliance.

SNPA v4.0—7-25

The security appliance gains dramatic performance advantages because of cut-through proxy: a method of transparently verifying the identity of users at the security appliance and permitting or denying access to any TCP- or UDP-based application. This method eliminates the price and performance impact that UNIX system-based firewalls impose in similar configurations, and leverages the authentication and authorization services of the Cisco Secure ACS.

The security appliance's cut-through proxy challenges a user initially at the application layer, then authenticates against standard TACACS+, RADIUS, or local databases. After the policy is checked, the security appliance shifts the session flow, and all traffic flows directly and quickly between the server and the client while maintaining session state information.

To authenticate a cut-through proxy user, only FTP, Telnet, HTTP, and HTTPS sessions can be intercepted.

- Telnet: You get a prompt generated by the security appliance. You have up to four chances to log in. If the username or password fails after the fourth attempt, the security appliance drops the connection.

- FTP: You get a prompt from the FTP program. If you enter an incorrect password, the connection is dropped immediately.

- HTTP: You see a window generated by the web browser. If you enter an incorrect password, you are prompted again.

- HTTPS: You get a prompt generated by the security appliance. You have up to three chances to log in. If the username or password fails after the third attempt, the security appliance drops the connection.

Keep in mind that browsers cache usernames and passwords. If you believe that the security appliance should be timing out an HTTP or HTTPS connection but it is not, reauthentication may actually be taking place, with the web browser sending the cached username and password back to the security appliance. If Telnet and FTP seem to work normally, but HTTP and HTTPS connections do not, this is usually why. The syslog service will show this phenomenon.

Cut-through Proxy User Authentication: Configuration Steps

Authentication configuration steps:

- **Specify an AAA server group.**

```
fw1(config)# aaa-server <server-tag> protocol <protocol>
```

- **Designate an authentication server.**

```
fw1(config)# aaa-server <server-tag> <(if_name)> host
<ip_address>
```

- **Enable cut-through proxy user authentication.**

```
fw1(config)# aaa authentication match <access_list_name>
```

  Or

```
fw1(config)# aaa authentication {include | exclude}
```

Configuring cut-through proxy authentication is a three-step process. The three steps are as follows:

Step 40 Specify an AAA server group. The administrator defines a group name and the authentication protocol.

Step 41 Designate an authentication server. The administrator defines the location of the AAA server and defines a key.

Step 42 Enable cut-through proxy user authentication. The administrator defines a rule to specify which traffic flow to authenticate.

Enable *authentication match*

Cisco.com
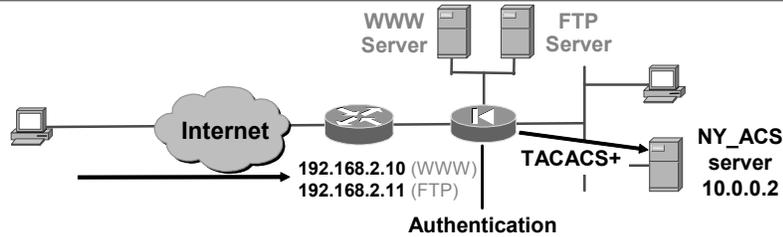
```
firewall (config)#
```

```
aaa authentication match acl_name if_name server_tag
```

- **Identify a traffic flow with an** access-list **command.**
- **Require authentication of traffic matching** access-list **command statement.**

```
fw1(config)# access-list 110 permit tcp any host 192.168.2.11 eq ftp
fw1(config)# access-list 110 permit tcp any host 192.168.2.10 eq www
fw1(config)# aaa authentication match 110 outside NY_ACS
```

SNPA v4.0—7-27

The **aaa authentication** command enables or disables user authentication services. With AAA authentication enabled, when you start a connection via Telnet, FTP, HTTP, or HTTPS, you are prompted for a username and password. An AAA server, previously designated with the **aaa-server** command, verifies whether the username and password are correct. If they are correct, the security appliance's cut-through proxy permits further traffic between the initiating host and the target host.

The **aaa authentication** command is not intended to mandate your security policy. The AAA servers determine whether a user can access the system, which services can be accessed, and which IP addresses can be accessed. The security appliance interacts with Telnet, FTP, HTTP, and HTTPS to display the prompts for logging. You can specify that a range of hosts or a single host be authenticated. You can set the **aaa authentication** command to a specific host and let the AAA server authenticate the user. You can set the local IP address in the **aaa authentication** command to **any** to mean all hosts and let the authentication server decide which hosts are authenticated. The AAA server enforces the security appliance AAA authentication policy.

For each IP address, one **aaa authentication** command is permitted for inbound connections and one is permitted for outbound connections. The security appliance permits only one authentication type per network. For example, if one network connects through the security appliance using TACACS+ for authentication, another network connecting through the security appliance can authenticate with RADIUS, but a single network cannot authenticate with both TACACS+ and RADIUS. In the example in the figure, any inbound FTP session to 192.168.2.11 and any inbound HTTP session to 192.168.2.10 is intercepted by the security appliance and authenticated by the AAA server. An AAA server from the NY_ACS group verifies the authentication username and password. After authentication, the session is cut through the security appliance.

Note   For cut-through proxy authentication, the administrator can also use the local security appliance user authentication database by specifying **LOCAL** for *server_tag*.

The syntax for the **aaa authentication** commands is as follows:

```
aaa authentication match acl_name if_name server_tag
```

acl-name	Specifies an **access-list** command statement name.
if_name	Interface name from which users require authentication. Use *if_name* in combination with *local_ip* and *foreign_ip* to determine from where access is sought and to where access is sought. The local IP address is always on the interface with the highest security level and the foreign IP address is always on the lowest.
server_tag	The server tag that is set with the **aaa-server** command. To use the local security appliance user authentication database, enter **LOCAL** for this parameter.

aaa authentication match Example
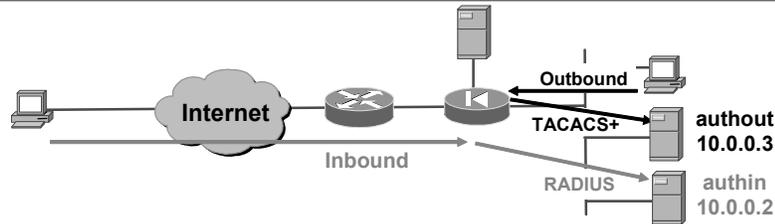
```
fw1(config)# aaa-server authin protocol radius
fw1(config)# aaa-server authin (inside) host 10.0.0.2
fw1(config-aaa-server)# key cisco123
fw1(config)# aaa-server authout protocol tacacs+
fw1(config)# aaa-server authout (inside) host 10.0.0.3
fw1(config-aaa-server)# key cisco456
fw1(config)# access-list 110 permit tcp any any eq telnet
fw1(config)# access-list 110 permit tcp any any eq ftp
fw1(config)# access-list 110 permit tcp any any eq www
fw1(config)# aaa authentication match 110 outside authin
fw1(config)# aaa authentication match 110 inside authout
```

SNPA v4.0—7-28

Authentication can be performed on the successful match of an ACL entry. This gives the administrator complete control of the cut-through authentication performed by the security appliance. It can be as selective or permissive as necessary. In the example in the figure, there are three ACL entries. The entries permit Telnet, FTP, and HTTP from any host to any host. The security appliance will intercept any sessions matching the ACL entries received on the outside interface. The cut-through proxy users are authenticated by an AAA server. In the example in the figure, there are two traffic flows, inbound and outbound. Any inbound traffic that matches the ACLs is authenticated by the authin AAA server using the RADIUS protocol. Any outbound traffic matching the ACL is authenticated by the authout AAA server using the TACACS+ protocol.

Enable *authentication include | exclude*

Cisco.com
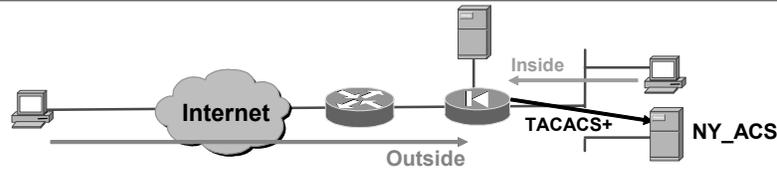
firewall (config)#

```
aaa authentication include | exclude authentication-service
  interface-name local-ip local-mask [foreign-ip foreign-mask]
  server-tag
```

• **Defines traffic to be authenticated: telnet, ftp, http, and https.**

```
fw1(config)# aaa authentication include ftp outside 0.0.0.0
  0.0.0.0 0.0.0.0 0.0.0.0 NY_ACS
fw1(config)# aaa authentication include telnet outside 0.0.0.0
  0.0.0.0 0.0.0.0 0.0.0.0 NY_ACS
fw1(config)# aaa authentication include http inside 0.0.0.0
  0.0.0.0 0.0.0.0 0.0.0.0 NY_ACS
fw1(config)# aaa authentication include https inside 0.0.0.0
  0.0.0.0 0.0.0.0 0.0.0.0 NY_ACS
```

SNPA v4.0—7-29

Another way to authenticate cut-through proxy users is the **aaa authentication include | exclude** command. The **aaa authentication include | exclude** command enables the administrator to stipulate which traffic flows to include or exclude in cut-through proxy user authentication. The **include** keyword creates a new rule with the specified service to include in authentication. The **exclude** keyword creates an exception to a previously stated rule by excluding the specified service from authentication.

The syntax for the **aaa authentication include | exclude** commands is as follows:

```
aaa authentication include | exclude authen_service if_name local_ip
 local_mask foreign_ip foreign_mask server_tag
```

```
no aaa authentication [include | exclude authen_service if_name
 local_ip local_mask foreign_ip foreign_mask server_tag]
```

```
clear aaa [authentication include | exclude authen_service if_name
 local_ip local_mask foreign_ip foreign_mask server_tag]
```

include	Creates a new rule to include a specified service.
exclude	Creates an exception to a stated rule by excluding the specified service from authentication to the specified host. The **exclude** parameter improves the former **except** option by enabling the user to specify a port to exclude to a specific host or hosts.
authen_service	The services that require user authentication before they are let through the security appliance. Use **any**, **ftp**, **http**, **https**, or **telnet**.
if_name	Interface name from which users require authentication. Use *if_name* in combination with *local_ip* and *foreign_ip* to determine to where access is sought and from where access is sought. The local IP address is always on the interface with the highest security level and the foreign IP address is always on the lowest.
local_ip	The IP address of the host or network of hosts that you want to be authenticated. You can set this address to **0** to mean all hosts.
local_mask	Network mask of the local IP address. Always specify a mask value. Use **0** if the IP address is 0. Use **255.255.255.255** for a host.
foreign_ip	The IP address of the hosts that you want to be able to access the local IP address. Use **0** to mean all hosts.
foreign_mask	Network mask of the foreign IP address. Always specify a mask value. Use **0** if the IP address is 0. Use **255.255.255.255** for a host.
server_tag	The server tag that is set with the **aaa-server** command. To use the local security appliance user authentication database, enter **LOCAL** for this parameter.

Show Authentication

"aaauser"
192.168.2.10

Internet

Outside

TACACS+

10.0.1.10
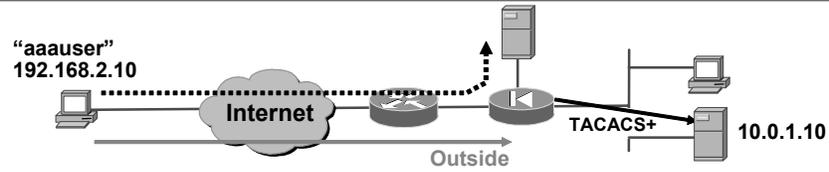
```
fw1(config)# show uauth
                     Current     Most Seen
Authenticated Users     1           1
Authen In Progress      0           1
user 'aaauser' at 192.168.2.10, authenticated
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
```

SNPA v4.0—7-30

Use the **show uauth** command to display one or all currently authenticated users, the host IP to which they are bound, and any cached IP and port authorization information. In the example in the figure, aaauser with an IP address of 192.168.2.10 is authenticated.

show *aaa-server* Command—TACACS+ Server

192.168.2.10

Internet

Outside

TACACS+

NY_ACS
Server
10.0.1.10
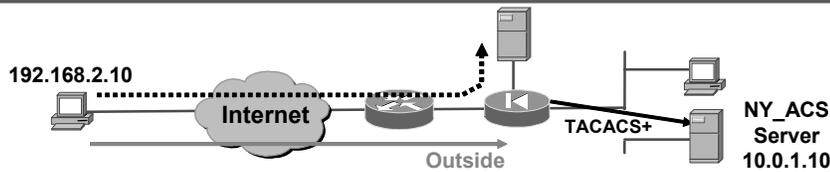
```
fw1# show aaa-server ny_acs
Server Group:    ny_acs
Server Protocol: tacacs+
Server Address:  10.0.1.10
Server port:     49
Server status:   ACTIVE, Last transaction at 16:17:23 UTC Mon
  Nov 29 2004
Number of pending requests           0
Average round trip time              3ms
Number of authentication requests    2
Number of authorization requests     0
Number of accounting requests        0
Number of retransmissions            0
Number of accepts                    2
Number of rejects                    0
Number of challenges                 2
```

SNPA v4.0—7-31

To display AAA server statistics for all configured server groups or for a particular group, use the **aaa-server** command. In the example in the figure, the top portion displays the server statistics; the bottom portion displays the server messaging statistics; and the server group is NY_ACS. It uses TACACS+ protocol, has an IP address of 10.0.1.10, uses server port number 49 for messaging, and is active. There are two requests, two challenges, and two accept messages.

Authentication of Non-Telnet, FTP, or HTTP Traffic

Cisco.com

Internet

PIX virtual authentication

Cisco Secure ACS server 10.0.0.2

Session with server

Server 10.0.0.33
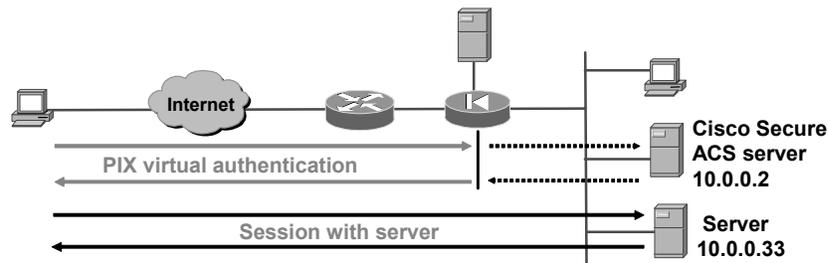
Authenticate to the Security Appliance before accessing other services.
  – **Virtual Telnet**
  – **Virtual HTTP**

SNPA v4.0—7-32

The security appliance authenticates users via Telnet, FTP, HTTP, or HTTPS. But what if users need to access a Microsoft file server on port 139 or a Cisco IP/TV server? How will they be authenticated? Whenever users are required to authenticate to access services other than by Telnet, FTP, HTTP, or HTTPS, they need to do one of the following:

■ **Option 1**: Authenticate first by accessing a Telnet, FTP, HTTP, or HTTPS server before accessing other services.

■ **Option 2**: Authenticate to the security appliance virtual Telnet service before accessing other services. When there are no Telnet, FTP, HTTP, or HTTPS servers with which to authenticate, or just to simplify authentication for the user, the security appliance allows a virtual Telnet authentication option. This option permits the user to authenticate directly with the security appliance using the virtual Telnet IP address.

Virtual Telnet

Cisco.com

192.168.9.10   **192.168.0.0**

Internet

.3

```
C:\> telnet 192.168.0.9
LOGIN Authentication
Username: aaauser
Password: aaapass
Authentication Successful
```

Virtual
Telnet

.9   Authentication

Cisco Secure
ACS server
10.0.0.2

File server
10.0.0.33
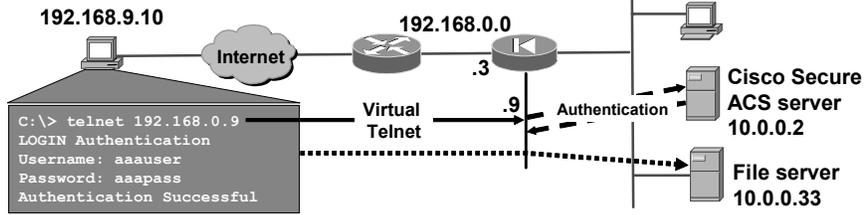
firewall (config)#

```
virtual telnet ip_address
```

- **Enables access to the Security Appliance's virtual server.**
  - **The IP address must be an unused global address.**

```
fw1(config)# access-list 120 permit tcp host 192.168.9.10 host 192.168.0.9
fw1(config)# aaa-server authin protocol radius
fw1(config)# aaa-server authin (inside) host 10.0.0.2
Fw1(config-aaa-server)# key cisco123
fw1(config)# aaa authentication match 120 outside authin
fw1(config)# virtual telnet 192.168.0.9
```

© 2005 Cisco Systems, Inc. All rights reserved.   SNPA v4.0—7-33

The virtual Telnet option provides a way to authenticate users who require connections through the security appliance using services or protocols that do not support authentication. When an unauthenticated user establishes a Telnet session to the virtual IP address, the user is challenged for the username and password, then authenticated with the TACACS+ or RADIUS server. Then the user sees the message "Authentication Successful," and the authentication credentials are cached in the security appliance for the duration of the user authentication (uauth) timeout.

If a user wishes to log out and clear the entry in the security appliance uauth cache, the user can again access the virtual address via Telnet. The user is prompted for a username and password, the security appliance removes the associated credentials from the uauth cache, and the user receives a "Logout Successful" message.

In the figure, the user wants to establish a Microsoft Internet Information Server (IIS) session to access the file server. The user accesses the virtual Telnet address at 192.168.0.9 and is immediately challenged for a username and password before being authenticated with the RADIUS AAA server. After the user is authenticated, the security appliance allows that user to connect to the file server without reauthentication.

The syntax for the **virtual telnet** command is as follows:

virtual telnet *ip_address*

ip_address	Unused global IP address on security appliance, used for Telnet for authentication.

Virtual HTTP

Cisco.com

PIX virtual HTTP authentication

Cisco Secure
ACS server
10.0.0.2

IIS authentication

IIS server
10.0.0.3
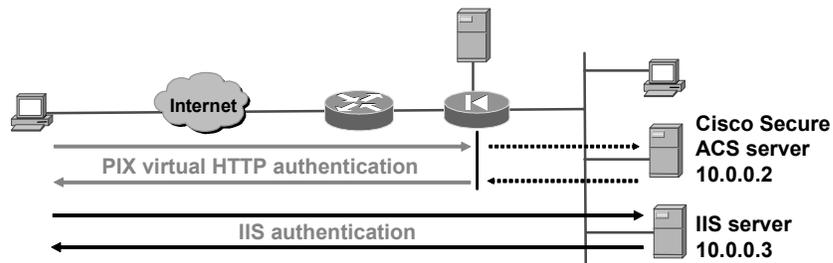
- **Virtual HTTP solves the problem of HTTP requests failing when web servers require credentials that differ from those required by the Security Appliance's AAA server.**
- **When virtual HTTP is enabled, it redirects the browser to authenticate first to a virtual web server on the Security Appliance.**
- **After authentication, the Security Appliance forwards the web request to the intended web server.**

SNPA v4.0—7-34

With the virtual HTTP option, web browsers work correctly with the HTTP authentication of the security appliance. The security appliance assumes that the AAA server database is shared with a web server and automatically provides the AAA server and web server with the same information. The virtual HTTP option works with the security appliance to authenticate the user, separate the AAA server information from the web client's URL request, and direct the web client to the web server. The virtual HTTP option works by redirecting the initial connection of the web browser to an IP address, which resides in the security appliance; authenticating the user; then redirecting the browser back to the URL that the user originally requested. The virtual HTTP option is so named because it accesses a virtual HTTP server on the security appliance.

This option is especially useful for security appliance interoperability with Microsoft IIS, but it is useful for other authentication servers as well. When using HTTP authentication to a site that is running Microsoft IIS and that has basic text authentication or Windows NT Challenge/Response authentication enabled, users may be denied access from the Microsoft IIS server because the browser appends the string "Authorization: Basic=Uuhjksdkfhk==" to the HTTP **GET** commands. This string contains the security appliance authentication credentials. Windows NT IIS servers respond to the credentials and assume that a Windows NT user is trying to access privileged pages on the server. Unless the security appliance username and password combination is exactly the same as a valid Windows NT username and password combination on the Microsoft IIS server, the HTTP **GET** command is denied.

To solve this problem, the security appliance redirects the browser's initial connection to its virtual HTTP IP address, authenticates the user, then redirects the browser to the URL that the user originally requested. Virtual HTTP is transparent to the user; therefore, users enter actual destination URLs in their browsers as they normally would.

Note Do not set the uauth time-out duration to 0 seconds when using the virtual HTTP option. Doing so prevents HTTP connections to the real web server.

Configuration of Virtual HTTP Authentication

192.168.0.0

.3

Virtual HTTP login

IIS HTTP login

Cisco Secure ACS server 10.0.0.2

IIS server 10.0.0.3

Virtual HTTP 192.168.0.8
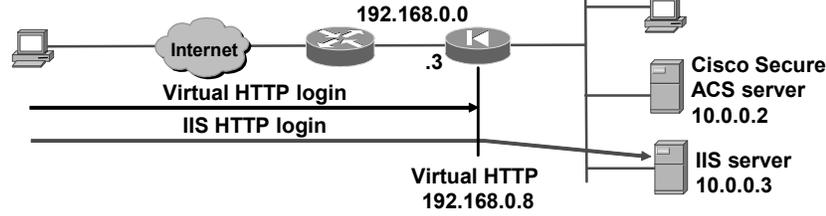
firewall (config)#

```
virtual http ip_address [warning]
```

- **For inbound clients, the IP address must be an unused global address.**
- **If the connection is started on either the outside or perimeter, a** static **and** access-list **command pair must be configured for the fictitious address.**

```
fw1(config)# virtual http 192.168.0.8
```

SNPA v4.0—7-35

The virtual address identifies the IP address of the virtual HTTP server on the security appliance. For inbound use, the IP address can be any unused global address. Access to this address must be provided by an **access-list** and **static** command pair. To be authenticated, the outside user establishes a virtual HTTP session to 192.168.0.8. The security appliance will intercept the virtual HTTP session and authenticate the user.

The syntax for the **virtual http** command is as follows:

```
virtual http ip_address [warn]
```

```
no virtual http ip_address
```

ip_address	The security appliance's network interface IP address.
warn	Informs **virtual http** command users that the command was redirected. This option is applicable only for text-based browsers in which the redirect cannot happen automatically.

Tunnel Access Authentication Configuration

This topic briefly discusses the configuration of security appliances for authorization.
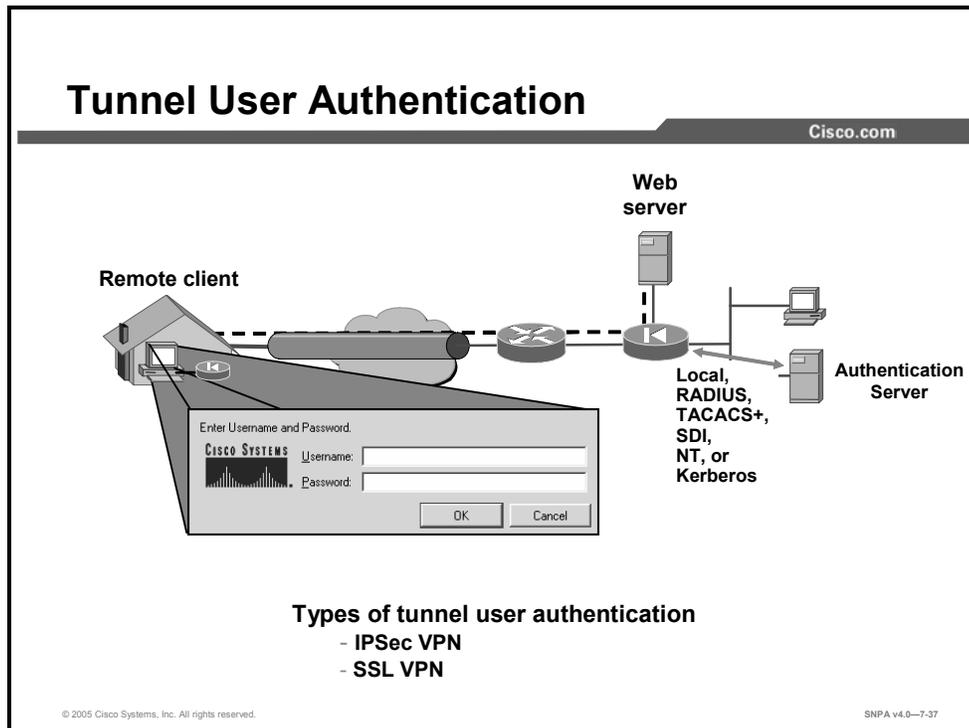
For tunnel access authentication, the security appliance can be configured to require remote tunnel users to authenticate prior to gaining access to the corporate services. The security appliance will prompt them for a username and password. The security appliance can authenticate users before fully establishing their tunnel.

VPN Tunnel Group Policy

Cisco.com

Push to client

Engineering Policy
Marketing Policy
Training Policy

Engineering

Training

Marketing

10.0.0.0 /24

Eng

Internet

Mktg

10.0.1.0/24

- VPN authentication can be defined by tunnel group.
- Different tunnel groups can authenticate to different authentication servers.

SNPA v4.0—7-38
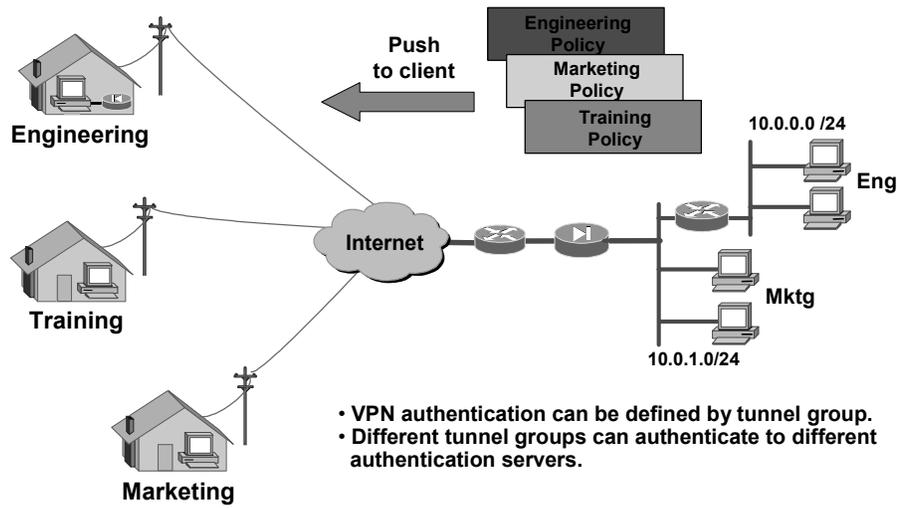
Each remote VPN user belongs to a specific VPN group or a default group. As users establish VPN tunnels to the central site security appliance, they authenticate. Through the authentication process, the security appliance identifies which group each remote user belongs to. The security appliance responds by pushing the appropriate VPN group policy to the remote user. In the figure, there are three VPN group policies configured: engineering, marketing, and training. Each VPN client belongs to one group.

Authorization Configuration

This topic discusses the configuration of Cisco security appliances for authorization.

Security Appliance User Authorization

Cisco.com

Two supported methods:
- **Classic user authorization, where a TACACS+ AAA server is configured with rules and consulted for every connection on demand**
- **Download of a per-user ACL from a RADIUS AAA server during authentication**

SNPA v4.0—7-40
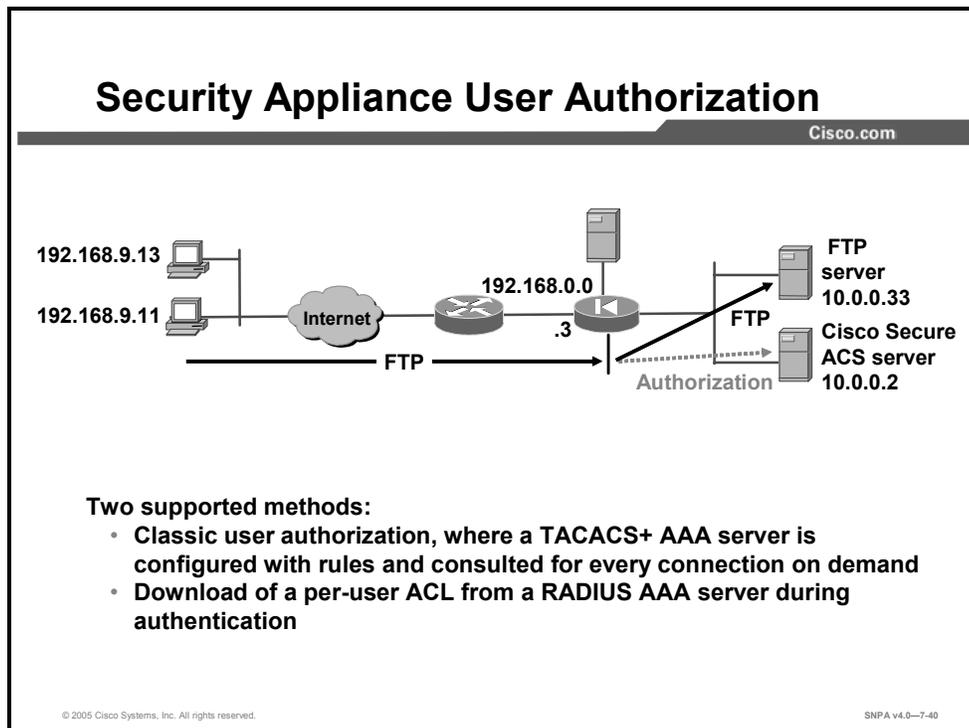
If you want to allow all authenticated users to engage in all operations—HTTP, HTTPS, FTP, and Telnet—through the security appliance, authentication is sufficient and authorization is not needed. But if there is reason to allow only some subset of users or to limit users to certain sites or services, authorization is needed. The security appliance supports two basic methods of user authorization when you specify per-user access rules in the context of AAA. These two methods are:

- Classic user authorization: The access rules are configured on the TACACS+ AAA server and consulted on demand. With classic authorization, the security appliance is configured with rules specifying which connections need to be authorized by the AAA server. The AAA server is consulted for access rights on demand. This functionality is supported only with TACACS+ servers.

- Download of per-user ACLs: Cisco PIX Security Appliance Software v6.2 introduced the ability to store full ACLs on the AAA server and download them to the security appliance. An ACL is attached to the user or group profile on the AAA server. During the authentication process, after the user's credentials are authenticated, the AAA server returns the ACL to the security appliance. The returned ACL is modified based on the source IP address of the authenticated user. This functionality is supported only with RADIUS.

TACACS+ Authorization Configuration

Two-step process to configure the aaa authorization **command**

- **Configure the Security Appliance**
  - **aaa authorization match**
  - **aaa authorization {include | exclude}**

- **Configure TACACS+ AAA server parameters**
  - **Commands**
  - **Arguments**

SNPA v4.0—7-41

User authorization is a two-step process. The administrator identifies the traffic flow to authorize, such as all FTP traffic flows, and configures the command authorization in the AAA server. The administrator can refine by group which set of users can access which corporate resources. The configuration steps are as follows:

Step 43   Configure the security appliance for authorization. The administrator can use the older **aaa authorization {include | exclude}** command or the newer **aaa authorization match** command.

Step 44   Define the AAA authorization group parameters on the TACACS+ server. The per-group command authorization parameters include commands and arguments.

Note   It is assumed that **aaa authentication** configuration is already completed.

Enable *authorization match*

Cisco.com

192.168.9.10   Internet   192.168.0.0   .3   FTP

FTP server
10.0.0.33

Cisco Secure
ACS server
10.0.0.2
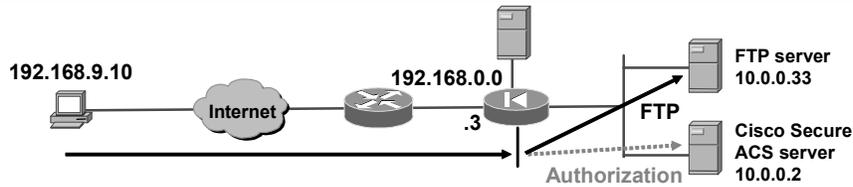
Authorization

firewall (config)#

```
aaa authorization match acl_name if_name server_tag
```

• **Identify a traffic flow with an ACL**
• **Define** aaa authorization match **statement in conjunction with a defined ACL.**

```
fw1(config)# access-list 101 permit tcp any any eq telnet
fw1(config)# access-list 101 permit tcp any any eq ftp
fw1(config)# access-list 101 permit tcp any any eq www
fw1(config)# aaa authorization match 101 outside authin
```

SNPA v4.0—7-42

Beginning in Cisco PIX Security Appliance Software v5.2, the administrator can define ACLs on the security appliance, then apply them to the **aaa authorization match** command. Any sessions that match the ACL must be authorized by the defined TACACS+ server group. In the example in the figure, the three ACL statements are for any-to-any FTP, Telnet, and HTTP traffic. The ACL is applied to the **aaa authorization** command for connection originating from the outside interface. Any inbound traffic on the outside interface that matches these characteristics must be authorized by authin TACACS+ server group.

Enable *authorization include | exclude*
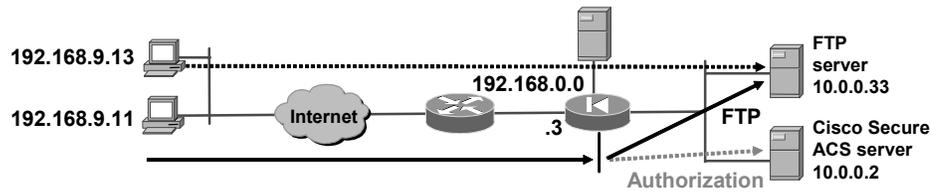
Cisco.com

```
firewall (config)#
```
```
aaa authorization {include | exclude} author_service  if_name
  local_ip local_mask foreign_ip foreign_mask server_tag
```

- **Identify the service to authorize.**
- **Define traffic that requires AAA server authorization.**
  - **Can't mix include | exclude and match authorization commands.**

```
fw1(config)# aaa authorization include ftp outside 0.0.0.0
  0.0.0.0 0.0.0.0 0.0.0.0 authin
fw1(config)# aaa authorization exclude ftp outside
  192.168.9.13 255.255.255.255 0.0.0.0 0.0.0.0 authin
```

© 2005 Cisco Systems, Inc. All rights reserved.   SNPA v4.0—7-43

The **aaa authorization** command defines which services require authorization. If the traffic matches the source and destination IP addresses and services in the **aaa authorization include** command string, the connection must be authorized by the defined TACACS+ AAA server. Services not specified in the command line are authorized implicitly.

In the example in the figure, any inbound FTP sessions must be authorized, with the exception of FTP sessions originating from IP address 192.168.9.13. If authentication passes and authorization is configured, the security appliance forwards the user's session information to the TACACS+ server for authorization. The TACACS+ returns a permit or fail message.

The syntax for the **aaa authorization** commands is as follows:

```
aaa authorization {include | exclude} author_service if_name local_ip
 local_mask foreign_ip foreign_mask server_tag
```

```
no aaa authorization include | exclude author_service if_name local_ip
 local_mask foreign_ip foreign_mask server_tag
```

include *author_service*	The services that require authorization. Use **any**, **ftp**, **http**, or **telnet**. Services that are not specified are authorized implicitly and do not require authorization. Services that are specified in the **aaa authentication** command do not affect the services that require authorization.
exclude *author_service*	Creates an exception to a previously stated rule by excluding the specified service from authorization to the specified host. The **exclude** parameter improves the former **except** option by allowing the user to specify a port to exclude for a specific host or hosts.
if_name	Interface name from which users require authorization. Use *if_name* in combination with *local_ip* and *foreign_ip* to determine where access is sought and by whom.
local_ip	The IP address of the host or network of hosts that you want to be authorized. You can set this address to **0** to mean all hosts.

local_mask	Network mask of the local IP address. Always specify a mask value. Use **0** if the IP address is 0. Use **255.255.255.255** for a host.
foreign_ip	The IP address of the hosts that you want to be able to access the local IP address. Use **0** to mean all hosts.
foreign_mask	Network mask of the foreign IP address. Always specify a mask value. Use **0** if the IP address is 0. Use **255.255.255.255** for a host.
server_tag	The server tag that is set with the **aaa-server** command.

Authorization Rules Allowing Specific Services

Per-group setup

Command authorization
- **Unmatched Security Appliance commands**
  - **Deny**
- **Command**
  - **ftp**
- **Arguments**
  - **None**
- **Unlisted arguments**
  - **Permit**

SNPA v4.0—7-44

The security appliance **aaa authorization** command defines which traffic flows to authorize. Clicking the Group Setup button, then selecting the Per Group Command Authorization radio button in the Cisco Secure ACS enables the administrator to permit or deny specific security appliance commands and arguments at the group level. For example, the Executive group might have FTP and HTTP access to all 172.26.26.0/24 servers. The Human Resources group might have FTP and HTTP access to server 172.26.26.50 only. The Per Group Command Authorization option enables the administrator to define authorization for commands, such as FTP, Telnet, and HTTP. It also enables the administrator to define authorization for arguments, such as server IP addresses.

To set TACACS+ authorization on a command-by-command basis, select **Per Group Command Authorization**, then select from the following options:

■ Unmatched Cisco IOS commands: To determine how Cisco Secure ACS handles commands that the administrator did not specify in this section, you can choose to either permit or deny, as applicable.

■ Command: You can select the Command check box and type the command in the field below it.

■ Arguments: For each argument of the command, you can specify whether the argument is to be permitted or denied.

■ Unlisted arguments: To permit only those arguments listed, select the Deny option. To allow users to issue all arguments not specifically listed, select the Permit option.

In the example in the figure, a member of a group is authorized to access any IP address via FTP. Complete the following steps to add authorization rules for this specific service in Cisco Secure ACS:

Step 45 Click **Group Setup** from the navigation bar. The Group Setup window opens.

Step 46 Scroll down to the Shell Command Authorization Set area under the TACAS+ settings section.

Step 47   Select **Per Group Command Authorization**, which enables the administrator to permit or deny specific command and arguments at the group level.

Step 48   Select **Deny**, which is found under Unmatched Cisco IOS commands. **Deny** allows only group members to issue FTP commands.

Step 49   Select **Command**.

Step 50   In the command field, enter **FTP**, the allowable service.

Step 51   Leave the Arguments field blank.

Step 52   Select **Permit**, which is found under Unlisted arguments, to permit the arguments that are not listed.

Step 53   Click **Submit** to add more rules; click **Submit + Restart** when you are finished.

Authorization Rules Allowing Specific Services to Specific Hosts

SNPA v4.0—7-45

Complete the following steps to add authorization rules for services to specific hosts in Cisco Secure ACS:

Step 54   Click **Group Setup** from the navigation bar. The Group Setup window opens.

Step 55   Scroll down in Group Setup to the Shell Command Authorization Set area.

Step 56   Select **Per Group Command Authorizatio**n.

Step 57   Select **Deny**, which is found under Unmatched Cisco IOS commands. When the administrator selects **Deny**, the user can issue only listed commands.

Step 58   Select **Command**.

Step 59   In the field below the check box, enter one of the allowable services.

Step 60   In the Arguments field, enter the IP addresses of the host that users are authorized to go to. Use the following format:

```
permit ip_addr
```

(where *ip_addr* = the IP address of the host)

Step 61   Select **Deny**, which is found under Unlisted arguments, to deny unlisted arguments.

Step 62   Click **Submit** to add more rules; click **Submit + Restart** when you are finished.

In the example in the figure, FTP to 172.26.26.50 is authorized for this group. All other destinations are denied.

Authorization of Non-Telnet, FTP, HTTP, or HTTPS Traffic

Cisco.com

firewall (config)#

```
aaa authorization {include | exclude} author_service if_name
  local_ip local_mask foreign_ip foreign_mask server_tag
```

- *author_service* = **protocol or port**
  - **protocol: tcp (6), udp (17), icmp (1), or others (protocol #)**
  - **Port number and message type:**
    - **Port number is used for TCP, UDP, or ICMP**
    - **Single port (e.g., 53), port range (e.g., 2000-2050), or port 0 (all ports)**
    - **ICMP message type (8 = echo request, 0 = echo reply)**

```
fw1(config)# aaa authorization include udp/0 outside 0.0.0.0
  0.0.0.0 0.0.0.0 0.0.0.0 authin
fw1(config)# aaa authorization include tcp/30-100 inside
  0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 authin
fw1(config)# aaa authorization include icmp/8 inside 0.0.0.0
  0.0.0.0 0.0.0.0 0.0.0.0 authin
```

SNPA v4.0—7-46

The authorization of non-Telnet, -FTP, -HTTP, -HTTPS is a two-step process. First, identify the traffic flows to be authorized. Next, define the group attributes in the TACACS+ AAA server. The syntax for the **aaa authorization** of non-Telnet, -FTP, -HTTP, and -HTTPS commands is as follows:

```
aaa authorization {include | exclude} author_service if_name local_ip
  local_mask foreign_ip foreign_mask server_tag
```

```
no aaa authorization [{include | exclude} author_service if_name
  local_ip local_mask foreign_ip foreign_mask server_tag
```

include *author_service*	The services that require authorization. Use a protocol and port number. Services that are not specified are authorized implicitly. Services that are specified in the **aaa authentication** command do not affect the services that require authorization. Use a port number of **0** to specify all ports.
exclude *author_service*	Creates an exception to a previously stated rule by excluding the specified service from authorization to the specified host or networks.
if_name	Interface name from which users require authentication. Use *if_name* in combination with *local_ip* and *foreign_ip* to determine where access is sought and from whom.
local_ip	The IP address of the host or network of hosts that you want to be authenticated or authorized. You can set this address to **0** to mean all hosts.
local_mask	Network mask of the local IP address. Always specify a mask value. Use **0** if the IP address is 0. Use **255.255.255.255** for a host.
foreign_ip	The IP address of the hosts that you want to be able to access the local IP address. Use **0** to mean all hosts.
foreign_mask	Network mask of the foreign IP address. Always specify a mask value. Use **0** if the IP address is 0. Use **255.255.255.255** for a host.

server_tag	The server tag that is set with the **aaa-server** command.

Authorization of Non-Telnet, FTP, or HTTP Traffic on Cisco Secure ACS

Cisco.com

Per-group setup

Command authorization

- **Unmatched PIX commands**
    - **Deny**
- **Command**
    - **1/8**
- **Arguments**
    - **None**
- **Unlisted arguments**
    - **Permit**

SNPA v4.0—7-47
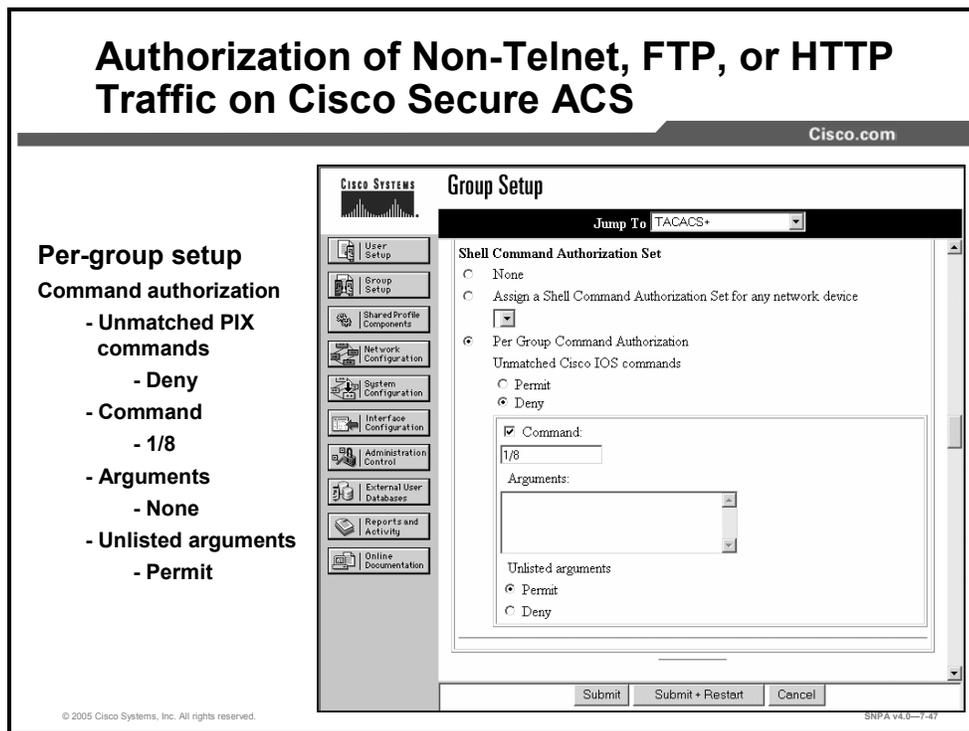
Complete the following steps to add authorization rules for specific non-Telnet, -FTP, -HTTP, or -HTTPS services to any group in Cisco Secure ACS:

Step 63   Click **Group Setup** on the navigation bar. The Group Setup window opens.

Step 64   Scroll down in Group Setup window to the Shell Command Authorization Set area.

Step 65   Select **Per Group Command Authorization**.

Step 66   Select **Deny**, which is found under Unmatched Cisco IOS commands.

Step 67   Select **Command**.

Step 68   In the field below the Command check box, enter an allowable service using the following format:

```
protocol/port
```

(where *protocol* = the protocol number, and *port* = the port number)

Step 69   Leave the Arguments field blank.

Step 70   Select **Permit**, which is found under Unlisted arguments.

Step 71   Click **Submit** to add more rules; click **Submit + Restart** when you are finished.

Downloadable ACLs

This topic describes the advantages of downloadable ACLs and explains how to configure them.

Security Appliance Downloadable ACL Authorization

Cisco.com

Downloadable ACLs:
- **Authentication request to AAA server**
- **Authentication response containing ACL**
- **ACL download of a per-user or per-group ACL authorization**

SNPA v4.0—7-49
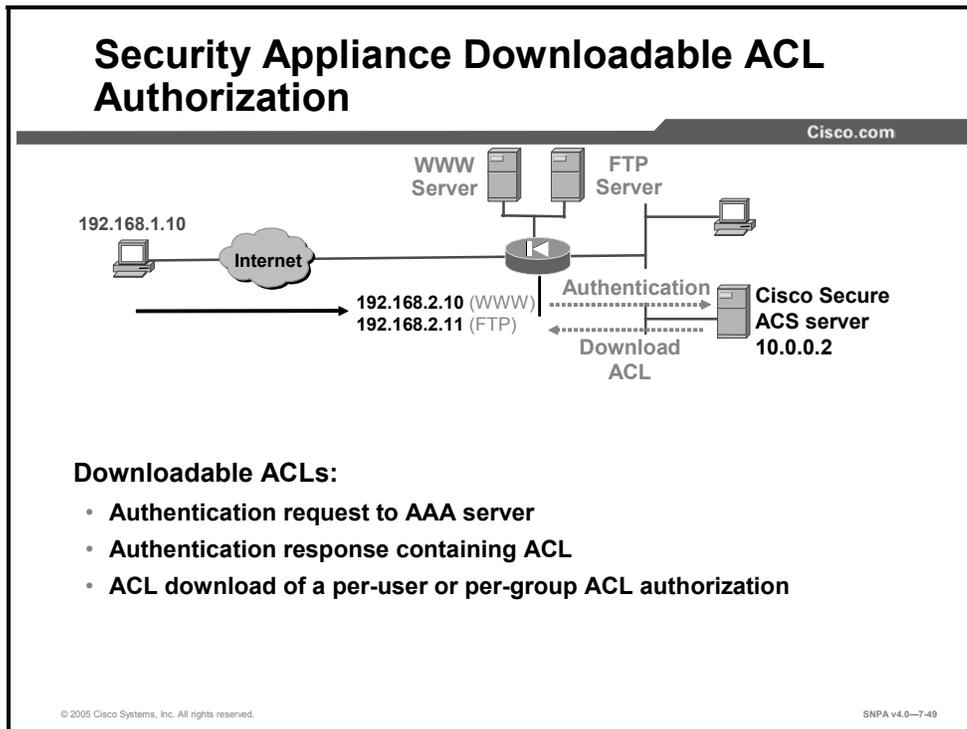
Cisco PIX Security Appliance Software v6.2 introduced the ability to store ACLs on the AAA server and download them to the security appliance as a user is authenticated. The security appliance permits or denies access based on the authentication of user credentials and the downloaded ACL. Users are authorized to do only what is permitted in their individual or group ACL entries. Authentication needs to be configured on the security appliance, and an ACL needs to be attached to the user or group profile on the AAA server. The security appliance supports per-user or per-group ACL authorization.

Note	Downloadable ACLs are supported with RADIUS only. They are not supported with TACACS+.

Downloadable ACLs

1. The HTTP request to Global IP address 192.168.1.10 is intercepted by the Security Appliance.
2. An authentication request is sent to AAA server.
3. The authentication response contains the ACL name from AAA server.
4. The Security Appliance checks to see if the user's ACL is already present.
5. A request is sent from the Security Appliance to the AAA server for the user's ACL.
6. The ACL is sent to the Security Appliance.
7. The HTTP request is forwarded to the WWW server.

192.168.0.10

Security Appliance

AAA server 172.16.1.4

W W W Server 10.0.1.11
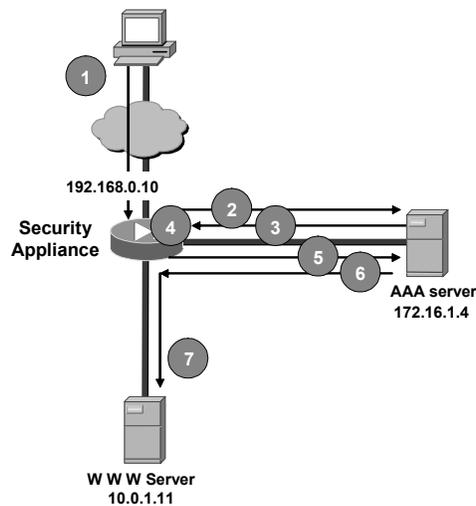
SNPA v4.0—7-50

Downloadable ACLs enable you to enter an ACL once in Cisco Secure ACS, then load that ACL to any number of security appliances. Downloadable ACLs work in conjunction with ACLs that are configured directly on the security appliance and applied to its interfaces. Neither type of ACL takes precedence over the other. In order to pass through the security appliance, traffic must be permitted by both the interface ACL and the dynamic ACL if both are applicable. If either ACL denies the traffic, the traffic is prohibited.

Downloadable ACLs are applied to the interface from which the user is prompted to authenticate. They expire when the uauth timer expires and can be removed using the **clear uauth** command.

As shown in the figure, the following sequence of events takes place when named downloadable ACLs are configured and a user attempts to establish a connection through the security appliance:

9. The user initiates a connection to the web server at 172.26.26.50. The application connection request is intercepted by the security appliance, which then interacts with the user to obtain the username and password.

10. The security appliance builds a RADIUS request that contains the user identification and password and sends it to the AAA server.

11. The AAA server authenticates the user and retrieves from its configuration database the ACL name associated with the user. The AAA server then builds a RADIUS response packet that contains the ACL name and sends it to the security appliance.

12. The security appliance checks to see if it already has downloaded the named ACL. A downloadable ACL is not downloaded again as long as it exists on the security appliance. Furthermore, to keep ACLs synchronized between a security appliance and an AAA server, the AAA server downloads to the security appliance a version identification along with the ACL name. This practice enables the security appliance to determine whether it needs to request an updated ACL.

13. If the named ACL is not present, the security appliance uses the name as a user identification and a null password to build a RADIUS access request. The security appliance then sends the RADIUS access request to the AAA server.

14. The AAA server retrieves from its configuration database the ACL associated with the ACL name. The AAA server then builds a RADIUS response packet containing the ACL and sends it to the security appliance.

15. The security appliance extracts the ACL and applies the dynamic ACL to the interface. The decision to forward or drop the packet is based on reviewing the interface ACLs and the dynamic ACLs. In this example, the security appliance forwards the connection request to the application server. The user then connects and interacts with the application server.

The downloaded ACL appears on the security appliance as shown this sample output. The ACL name is the name for the ACL as defined in the shared profile component (SPC), and 3b5385f7 is a unique version identification.

```
access-list #ACSACL#-PIX-acs_ten_acl-3b5385f7 permit ftp any
host  172.26.26.50
access-list #ACSACL#-PIX-acs_ten_acl-3b5385f7 permit http any
host 172.26.26.50
```

Configuring Downloadable ACLs in Cisco Secure ACS

Cisco Systems

Shared Profile Components

Edit

Downloadable IP ACL Content

Name: radiusauth

ACL Definitions

```
permit tcp any host 192.168.1.10 eq ftp
permit tcp any host 192.168.1.11 eq ftp
permit tcp any host 192.168.1.10 eq www
permit tcp any host 192.168.1.11 eq www
deny ip any any
```

User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Reports and Activity
Online Documentation

Submit Delete Cancel

SNPA v4.0—7-51

There are two methods of configuring downloadable ACLs on the AAA server. The first method, downloading named ACLs, is to configure the SPC to include both the ACL name and the actual ACL, then configure a user or group authentication profile to include the SPC. If you configure a downloadable ACL as a named SPC, you can apply that ACL to any number of Cisco Secure ACS user or group profiles. This method should be used when there are frequent requests for downloading a large ACL.

The second method is to configure a user authentication profile on the AAA server that includes the actual security appliance ACL. In this case, the ACL is not identified by a name. You must define each ACL entry in the user profile. This method should be used when there are not frequent requests for the same ACL. For instructions on downloading ACLs without names, refer to the documentation on Cisco.com.

Complete the following steps on the AAA server to configure named downloadable ACLs:

Step 72 Choose **Interface Configuration > Advanced Options** from the main Cisco Secure ACS window to enable the Downloadable ACLs option. Within the Advanced Options group box, select the following:

- **User-Level Downloadable ACLs**

- **Group-Level Downloadable ACLs**

Step 73 Select **Downloadable IP ACLs** from the Shared Profile Components menu item.

Step 74 Click **Add** to add an ACL definition. Enter the name, description, and the actual definitions for the ACL.

The ACL definition consists of one or more security appliance **access-list** command statements, with each statement on a separate line. Each statement must be entered without the **access-list** keyword and without the *acl_ID* argument for the ACL. The rest of the command line must conform to the syntax and semantics rules of the security appliance **access-list** command. A security appliance syslog message is logged if there is an error in a downloaded **access-list** command. When you have finished specifying the ACL, click **Submit**.

Assigning the ACL to the User or Group

SNPA v4.0—7-52

After you have configured the downloadable ACL, configure a Cisco Secure ACS user or group through User Setup or Group Setup to include the defined ACL in the user or group settings.

Show Downloaded ACLs

WWW Server FTP Server

192.168.1.10

Internet

192.168.2.10 (WWW)
192.168.2.11 (FTP)

Authentication

Download
RADIUSAUTH ACL

Cisco Secure
ACS server
10.0.0.2
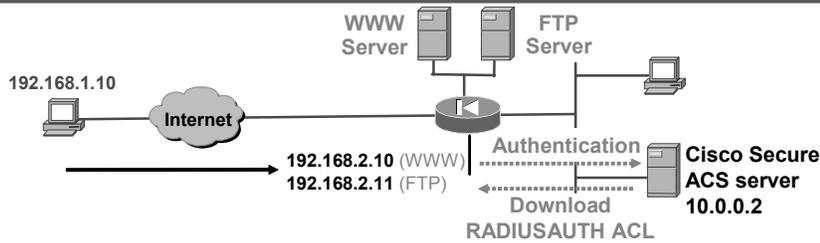
```
fw1# show access-list
…………….

access-list #ACSACL#-IP-RADIUSAUTH-3ddb8ab6; 3 elements
access-list #ACSACL#-IP-RADIUSAUTH-3ddb8ab6 line 1 extended
  permit tcp any host 192.168.2.10 eq www (hitcnt=5)
access-list #ACSACL#-IP-RADIUSAUTH-3ddb8ab6 line 2 extended
  permit tcp any host 192.168.2.11 eq ftp (hitcnt=0)
access-list #ACSACL#-IP-RADIUSAUTH-3ddb8ab6 line 3 extended
  deny ip any any (hitcnt=0)
```

SNPA v4.0—7-53

After a user is authenticated, the administrator can view the downloaded ACL using the **show access-list** command. In the example in the figure, the user at 192.168.1.10 attempts to gain access to the web server at 192.168.2.10. After end users enter their username and password, the security appliance forwards their credentials to the Cisco Secure ACS. If the end user is authenticated, the Cisco Secure ACS downloads a preconfigured ACL #ACSACL#-IP-RADIUSAUTH-3ddb8ab6 to the security appliance. The ACL name, #ACSACL#-IP-RADIUSAUTH, is the name for the ACL as defined in the SPC, and 3ddb8ab6 is a unique version identification. In this example, the end user is authorized to access 192.168.2.10 using HTTP.

Show Authentication
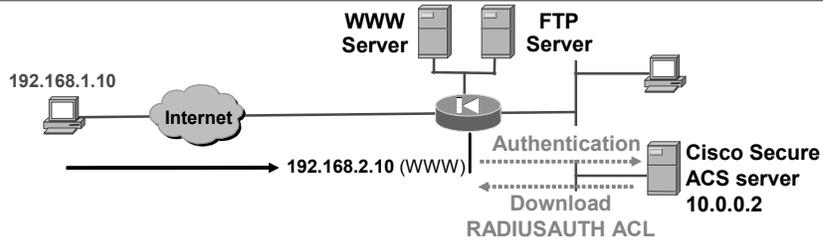
WWW Server   FTP Server

192.168.1.10

Internet

192.168.2.10 (WWW)

Authentication

Download
RADIUSAUTH ACL

Cisco Secure
ACS server
10.0.0.2

```
fw1# show uauth
                    Current    Most Seen
Authenticated Users    1          1
Authen In Progress     0          1
user 'aaauser' at 192.168.1.10, authenticated
   access-list #ACSACL#-IP-RADIUSAUTH-3ddb8ab6 (*)
 absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
```

SNPA v4.0—7-54

In the **show uauth** command, the administrator can view the authenticated end users, their IP addresses, and the matching downloaded ACL. In the example in the figure, end user aaauser at IP address 192.168.1.10 was authenticated. The matching ACL that was downloaded to the security appliance was named #ACSACL#-IP-RADIUSAUTH-3ddb8ab6. To view the actual ACL, the administrator can use the **show access-list** command.

show aaa-server Command—RADIUS

WWW Server   **FTP Server**

192.168.1.10

Internet

192.168.2.10 (WWW)

Authentication

Download ACL

Cisco Secure ACS server 10.0.0.2
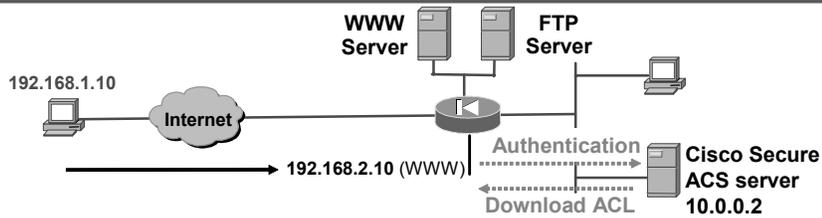
```
Fw1# show aaa-server
Server Group:    myradius
Server Protocol: radius
Server Address: 10.0.0.2
Server port:     1645(authentication), 1646(accounting)
Server status:   ACTIVE, Last transaction at 14:33:13 utc Thu Aug 26 2004
Number of pending requests           0
Average round trip time              30ms
Number of authentication requests    1
Number of authorization requests     0
Number of accounting requests        0
Number of retransmissions            0
Number of accepts                    1
Number of rejects                    0
Number of challenges                 1
Number of malformed responses        0
Number of bad authenticators         0
Number of timeouts                   0
Number of unrecognized responses     0
```

SNPA v4.0—7-55

The administrator can also view the AAA server messaging statistics. In the example in the figure, there was an authentication request, a challenge, and an accept message. There were no rejects or retransmissions.

Per-User_Override

WWW Server   FTP Server

192.168.1.10

Internet

192.168.2.10 (WWW)

Authentication

Cisco Secure ACS server 10.0.0.2
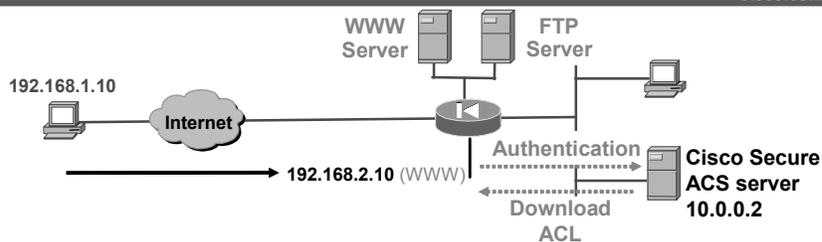
Download ACL

When *per-user-override* is present, the security appliance allows the **permit** or **deny** ACE from the downloaded per-user access-list to override the permit or deny ACE from the **access-group** command.

Existing access-list:
Permit tcp any any **eq www** (hitcnt=0)
Downloaded per-user access-list:
Deny tcp any host **192.168.2.10 eq www (hitcnt=1)**

```
fw1# show run access-group
access-group aclin in interface outside per-user-override
```

SNPA v4.0—7-56

When a user authenticates, an ACL is downloaded from the Cisco Secure ACS and is added to an existing ACL. When per-user override is present in the **access-group** command, the downloaded ACE can override the existing security appliance ACE for this access group. The per-user override enables the permit or deny ACE statement from the downloaded per-user ACL to override the permit or deny ACE statement from the **access-group** command. In the example in the figure, there are two ACL elements, permit any host access to any host via HTTP and deny any host access to 192.168.2.10 via HTTP. The first ACE is an existing ACE resident in the security appliance. The second is a downloadable ACE from the authentication server. When the user authenticates, the deny ACE associated with this user is downloaded to the security appliance. The downloaded ACE overrides the existing ACE in the security appliance. The deny ACE instructs the security appliance to block the inbound HTTP session to 192.168.2.10.

Per-User-Override Example
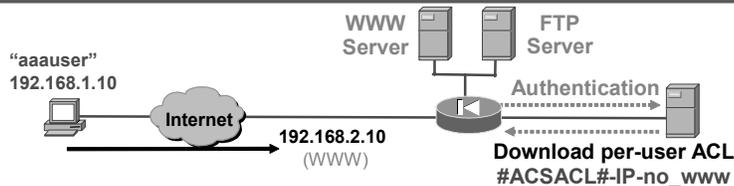
WWW Server FTP Server

"aaauser"
192.168.1.10

Internet

192.168.2.10
(WWW)

Authentication

Download per-user ACL
#ACSACL#-IP-no_www

```
fw1# show uauth
                        Current    Most Seen
Authenticated Users      1          1
Authen In Progress       0          1
user 'aaauser' at 192.168.1.10, authenticated
   access-list #ACSACL#-IP-no_www-41aef3fc (*)
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
fw1# show access-list
…………….
access-list aclin line 3 extended permit tcp any host 192.168.2.10
  eq www (hitcnt=2)
…………….
access-list aaa-www line 1 extended permit tcp any host 192.168.2.10
  eq www (hitcnt=4)
………….
access-list #ACSACL#-IP-no_www-41aef3fc line 2 extended deny tcp any
  host 192.168.2.10 eq www (hitcnt=1)
```

SNPA v4.0—7-57

The administrator can view the per-user override feature using the **show uauth** and **show access-list** commands. In the example in the figure, aaauser at 192.168.1.10 attempts to establish a session with the web server at 192.168.2.10. The first ACE permits HTTP traffic from any outside host to 192.168.2.10. The second ACE identifies which traffic flow must be authenticated. The session is intercepted by the security appliance, and the remote user is forced to authenticate. As part of the authentication process, a per-user ACL is downloaded to the security appliance, the third ACE element in the example in the figure. This ACE is a deny statement that overrides the existing permit statement. The remote user's session is blocked. Notice under the **show uauth** command in the example, aaauser was successfully authenticated. The **#ACSACL#-IP-no_www**-41aef3fc ACE was applied to the session. **#ACSACL#-IP-no_www**-41aef3fc ACE denies HTTP access to 192.168.2.10.

Accounting Configuration

This topic demonstrates how to enable and configure accounting for all services, specific services, or no services.
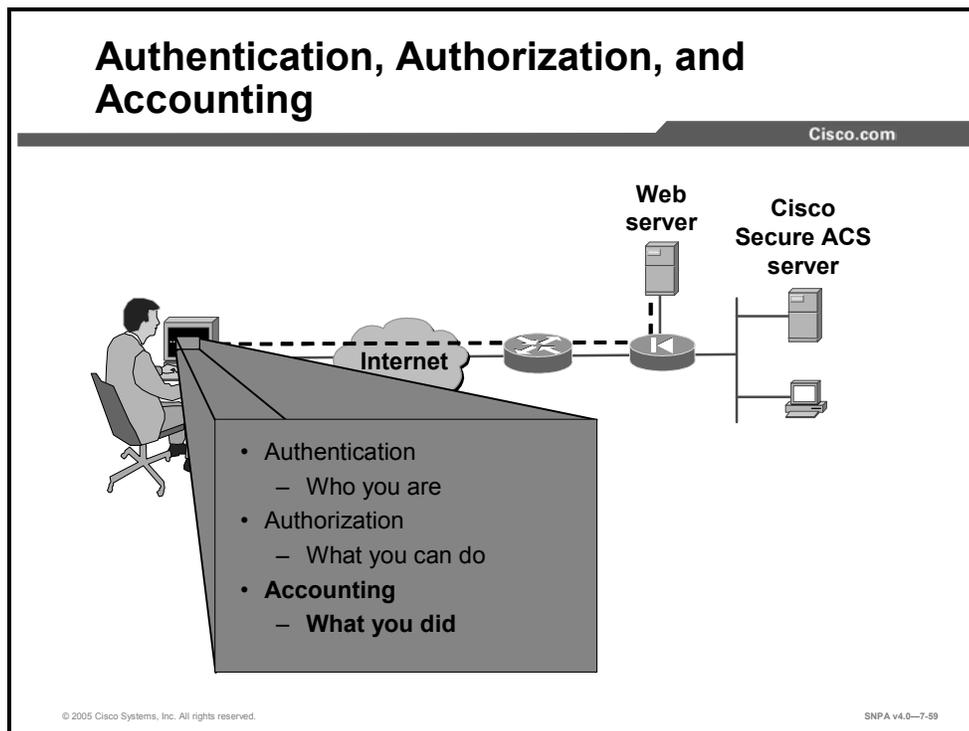
To enable, disable, or view user accounting (on a server designated by the **aaa-server** command), use the **aaa accounting** command. Accounting is provided for all services, or you can limit it to one or more services. User accounting services keeps a record of which network services a user has accessed. Accounting messages are sent to a single server if the AAA server group is configured for single mode. Accounting messages are sent to all servers in the group if the AAA server is configured for simultaneous mode. These accounting records are kept on the designated AAA server or servers. This command applies only to TACACS+ and RADIUS servers.

Enable *accounting match*

Cisco.com

Web server

Traffic Flow
- ftp   - http

Internet

Accounting

NY_ACS server
10.0.0.2
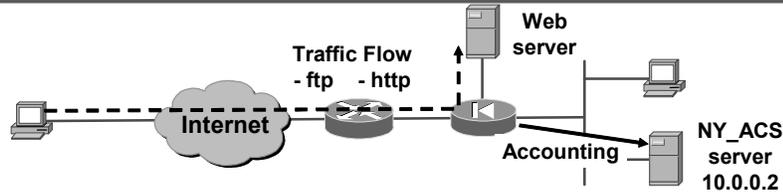
firewall (config)#

```
aaa accounting match acl_name interface_name server_tag
```

- **Identify a traffic flow with an** access-list **command.**
- **Enable accounting of traffic matching** access-list **command statement.**

```
fw1(config)# access-list 110 permit tcp any host 192.168.2.10 eq ftp
fw1(config)# access-list 110 permit tcp any host 192.168.2.10 eq www
fw1(config)# aaa accounting match 110 outside NY_ACS
```

SNPA v4.0—7-60

To enable the generation of an accounting record, the administrator identifies a traffic flow with an ACL and applies the ACL to the **aaa accounting match** command. In the example in the figure, the ACL 110 identifies the FTP and HTTP traffic flow from any host to the web server at IP address 192.168.2.10. The **match** *acl_name* option in the **aaa accounting match** command instructs the security appliance to generate an accounting record when the action that the user is trying to perform matches the actions specified in the ACL. Therefore, any time a user tries to access the web server via FTP or HTTP, an accounting record is generated and sent to the accounting server NY_ACS.

The syntax for the **aaa accounting match** command is as follows:

```
aaa accounting match acl_name if_name server_tag
```

match *acl_name*	Specifies an **access-list** command statement name.
if_name	Interface name from which users require authentication. Use *if_name* in combination with *local_ip* and *foreign_ip* to determine where access is sought and by whom.
server_tag	The group tab that is set with the **aaa-server** command. To use the local security appliance user authentication database, enter **LOCAL** for this parameter.

Enable *accounting include | exclude*
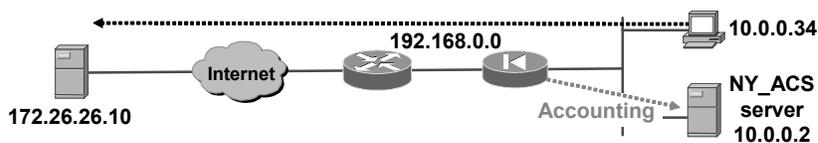
```
                                                       192.168.0.0            10.0.0.34

          Internet

172.26.26.10                                          Accounting         NY_ACS
                                                                         server
                                                                         10.0.0.2
```

firewall (config)#

```
aaa accounting {include | exclude} acctg_service if_name local_ip
  local_mask foreign_ip foreign_mask server_tag
```

- **Defines traffic that requires AAA server accounting.**
- **acctg_service = any, ftp, http, telnet, or protocol/port**
  - **any = All TCP traffic**

```
fw1(config)# aaa accounting include any inside 0.0.0.0
  0.0.0.0 0.0.0.0 0.0.0.0 NY_ACS
fw1(config)# aaa accounting exclude any inside 10.0.0.34
  255.255.255.255 0.0.0.0 0.0.0.0 NY_ACS
```

SNPA v4.0—7-61

User accounting records can be kept on a designated AAA server. Accounting information is sent only to the active server in a server group. Traffic that is not specified by an **include** statement is not processed. In the example in the figure, accounting records are kept on the AAA server for all outbound connections except for those connections originating from host 10.0.0.34.

The syntax for the **aaa accounting** commands is as follows:

```
aaa accounting{ include | exclude} acctg_service if_name local_ip
  local_mask foreign_ip foreign_mask server_tag
```

include *acctg_service*	The accounting service. Accounting is provided for all services, or you can limit it to one or more services. Possible values are **any**, **ftp**, **http**, **telnet**, or **protocol/port**. Use **any** to provide accounting for all TCP services. To provide accounting for UDP services, use **protocol/port**.
exclude *acctg_service*	Create an exception to a previously stated rule by excluding the specified service from accounting to the specified host. The **exclude** parameter improves the former **except** option by allowing the user to specify a port to exclude to a specific host or hosts.
if_name	Interface name from which users require accounting. Use *if_name* in combination with *local_ip* and *foreign_ip* to determine where access is sought and from whom.
local_ip	The IP address of the host or network of hosts that you want to enable for accounting. You can set this address to **0** to mean all hosts.
local_mask	Network mask of the local IP address. Always specify a specific mask value. Use **0** if the IP address is 0. Use **255.255.255.255** for a host.
foreign_ip	The IP address of the hosts that you want to be able to access the local IP address. Use **0** to mean all hosts.

foreign_mask	Network mask of the foreign IP address. Always specify a mask value. Use **0** if the IP address is 0. Use **255.255.255.255** for a host.
server_tag	The server tag that was set with the **aaa-server** command.

How to View Accounting Information in Cisco Secure ACS

Complete the following steps to add accounting rules in Cisco Secure ACS:

Step 75   Click **Reports and Activity** in the navigation bar. The Reports and Activity window opens.

Step 76   Click the RADIUS Accounting link to display the accounting records.

Accounting of Non-Telnet, FTP, or HTTP Traffic

firewall (config)#

```
aaa accounting {include | exclude} acctg_service if_name
  local_ip local_mask foreign_ip foreign_mask server_tag
```

- *acctg_service* = protocol or port
  - Protocol: tcp (6), udp (17), or others (protocol #)
  - Port = Single port (such as 53), port range (such as 2000–2050), or port 0 (all ports); port not used for protocols other than TCP or UDP

```
fw1(config)# aaa accounting include udp/53 outside
  0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 NY_ACS
fw1(config)# aaa accounting include udp/54-100 inside
  0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 NY_ACS
```

SNPA v4.0—7-63

To specify the value of the *acctg_service* argument using the protocol/port form, enter the protocol as a number (6 for TCP, 17 for UDP, 1 for ICMP, and so on). The port is the TCP or UDP destination port. A port value of 0 means all ports. If the specified protocol is ICMP, the port is the ICMP type, such as 8 for ICMP echo and 0 for ICMP echo-reply. Examples of the **aaa accounting** command using protocol/port form follow:

- **aaa accounting include 17/53 inside 0 0 0 0 authin**: Enables accounting for Domain Name System (DNS) lookups from the outside interface

- **aaa accounting include 1/0 inside 0 0 0 0 authout**: Enables accounting of ICMP echo-reply packets arriving at the inside interface from inside hosts

- **aaa accounting include 1/8 inside 0 0 0 0 authout**: Enables accounting only for ICMP echoes (pings) that arrive at the inside interface from an inside host

Admin Accounting

"student1"

Telnet

Internet
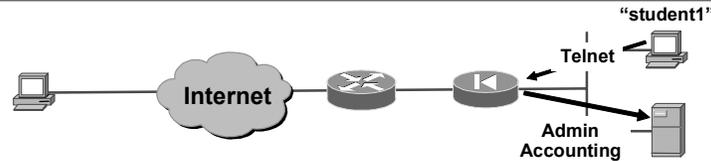
Admin
Accounting

firewall (config)#

```
aaa accounting {http | serial| telnet | ssh | enable} console
   server-tag
```

- **Enables or disables the generation of accounting records to mark the establishment and termination of admin sessions.**
- **Valid server group protocols are RADIUS and TACACS+.**

```
fw1(config)# username student1 password cisco123
fw1(config)# aaa authentication telnet console LOCAL
fw1(config)# aaa accounting telnet console NY_ACS
```

SNPA v4.0—7-64

The administrator can enable the generation of accounting records to mark the establishment and termination of security appliance console access. In the example in the figure, the username student1 and the password cisco123 are added to the security appliance local database. Next, the administrator configures the security appliance to authenticate all Telnet access sessions using the local database to authenticate users. Lastly, an accounting record is generated for each Telnet session. The record is sent to the NY_ACS.

The syntax for the **aaa accounting console** commands is as follows:

```
aaa accounting {http | serial| telnet | ssh | enable} console server-
tag
```

serial	Verifies access for the security appliance's serial console.
enable	Verifies access for the security appliance's privilege mode.
telnet	Verifies Telnet access to the security appliance console.
ssh	Verifies SSH access to the security appliance console.
http	Verifies HTTP access to the security appliance (via Cisco PIX Device Manager [PDM]).
console	Specifies that access to the security appliance console requires authentication.
server_tag	The server tag that is set with the **aaa-server** command. To use the local security appliance user authentication database, enter **LOCAL** for this parameter.

Viewing RADIUS Admin Access Accounting Information in Cisco Secure ACS

To view the accounting records, click on the Reports and Activity icon. Next select the proper link depending on the type of accounting record generated, TACACS+ or RADIUS. In the example in the figure, an accounting record was generated when student1 telnetted to the security appliance. Student1 accessed the security appliance using privilege level enable_15. The accounting records were generated when the student1 Telnet session began and when it terminated.

Command Accounting

"student1"

Telnet

Internet

Command Accounting
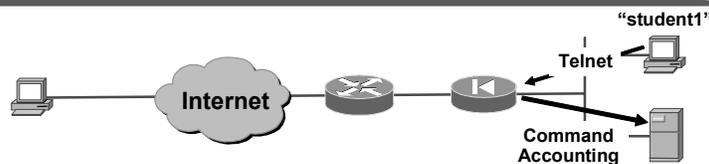
firewall (config)#

```
aaa accounting command [privilege level] server-tag
```

- **Enables or disables the generation of command accounting records for admin sessions.**
- **Valid server group protocol is TACACS+.**

```
fw1(config)# aaa accounting command privilege 6 mytacacs
```

SNPA v4.0—7-66

When you configure the **aaa accounting command** command, each command entered by an administrator and user is recorded and sent to the accounting server or servers. The optional **privilege** specification indicates the minimum privilege level that must be associated with a command for an accounting record to be generated. This command applies only to TACACS+ servers. You must specify the name of the server or group, previously specified in an **aaa-server** command, to which this command applies. In the example in the figure, the administrator configures the security appliance to record all changes to the configuration by people accessing the security appliance with privilege level 6 or higher.

The syntax for the **aaa accounting command** command is as follows:

```
aaa accounting command [privilege level] server-tag
```

server-tag	The server or group of TACACS+ servers to which accounting records are sent.
privilege *level*	The minimum level that must be associated with a command for an accounting record to be generated. The default privilege level is 0.

Viewing TACACS+ Admin Command Accounting Information

SNPA v4.0—7-67

The administrator configured the security appliance to record all changes to the configuration by people accessing the security appliance with privilege level 6 or higher. In the example in the figure, student1, with an access privilege level of 15, was authenticated. The TACACS+ server recorded student1 entering two **access-list** commands.

Summary

This topic summarizes what you have learned in this lesson.

Summary

Cisco.com

- **Authentication is who you are, authorization is what you can do, and accounting is what you did.**
- **Security appliance can authenticate the following:**
  - **Access to the security appliance via Telnet, SSH, serial, or enable.**
  - **Telnet, FTP, HTTPS, or HTTP traffic through the security Appliance.**
  - **IPSec and SSL VPN tunnel access.**
- **Downloadable ACLs enable you to enter an ACL once, in Cisco Secure ACS, and then download that ACL to any number of security Appliances during user authentication.**

SNPA v4.0—7-68

Lesson 8

Switching and Routing

Overview

This lesson explains the VLAN capabilities of Cisco security appliances, then continues with a discussion of their routing capabilities. It also covers: Routing Information Protocol (RIP) and Open Shortest Path First (OSPF); and configuring a security appliance to allow multicast traffic.

Objectives

Upon completing this lesson, you will be able to describe and configure the switching and routing functionality that your security appliance provides. This includes being able to meet these objectives:

- Describe the VLAN functionality of Cisco security appliances

- Explain the routing functionality of Cisco security appliances

- Configure a security appliance to work with RIP

- Configure a security appliance to work with OSPF

- Configure a security appliance to forward multicast traffic

VLANs

This topic explains the VLAN capabilities of Cisco security appliances.

VLANs

DMZ

Public Server | Partner Server | Proxy Server

VLAN

VLAN   VLAN

VLAN Trunk Port

Internet

Outside   Inside

- **Two physical LAN connections**
  - **Inside**
  - **Outside**
- **Three VLAN connections**
  - **DMZ servers**

SNPA v4.0—8-3
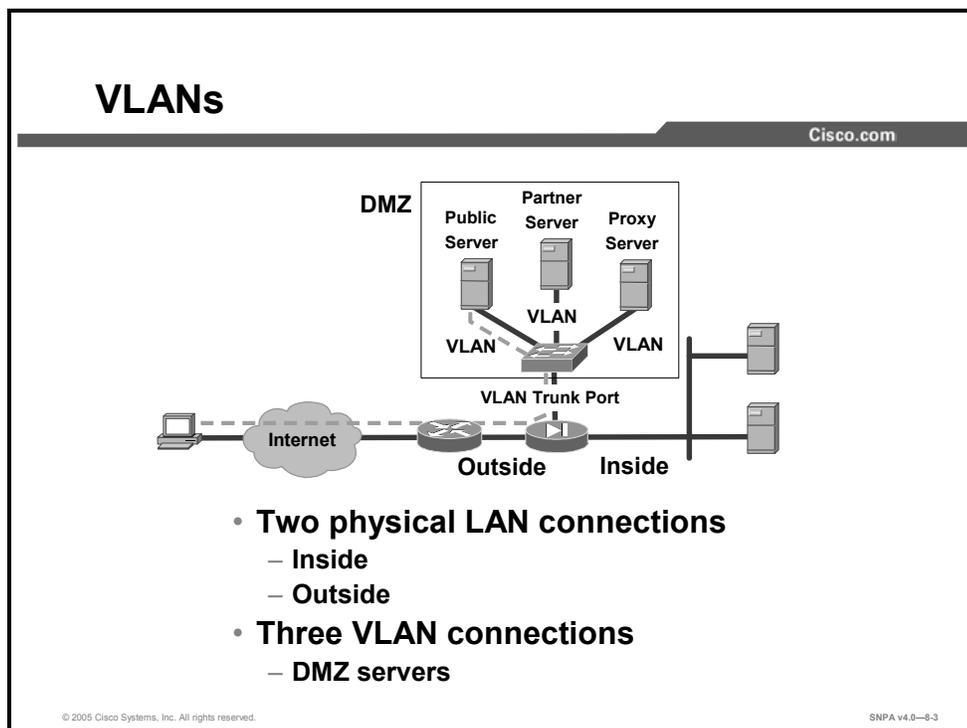
With Cisco PIX Security Appliance Software v6.3 and higher and Cisco PIX and ASA Security Appliance Software v7.0 and higher, the administrator can assign VLANs to physical interfaces on the security appliance or configure multiple logical interfaces on a single physical interface and assign each logical interface to a specific VLAN. A VLAN connects devices on one or more physical LAN segments so that the VLAN can act as though it is attached to the same physical LAN. VLANs make this connection based on logical (software) connections instead of physical connections, which makes them extremely flexible because you can configure and reconfigure which segments belong to which VLAN entirely through software.

Cisco PIX Series 500 Security Appliances (except for the 501, 506, and 506E) and Cisco ASA 5500 Series Adaptive Security Appliances support only 802.1q VLANs. Specifically, they support multiple 802.1q VLANs on a physical interface and the ability to receive and send 802.1q-tagged packets. VLANs are not supported on the Cisco PIX 501, 506, and 506E Security Appliances.

Cisco security appliances do not currently support executable commands for LAN trunks (the physical and logical connection between two switches) because the security appliances do not negotiate or participate in any bridging protocols. The security appliances display the VLANs only on the LAN trunk. It considers the state of the LAN trunk to be the same as the state of the physical interface. If the link is up on the physical Ethernet, then the security appliance considers the trunk as up as soon as a VLAN has been assigned or configured for it. Additionally, the VLAN is active as soon as you assign or configure a VLAN identifier (ID) on the physical Ethernet interface of the security appliance.

Physical interfaces are one per network interface card (NIC), in place at boot time, and not removable. Logical interfaces can be many-to-one for each NIC, are created at runtime, and can be removed through software reconfiguration. For VLANs to be supported, a minimum of two physical interfaces is required for all security appliance platforms.

Creating Logical and Physical Interfaces
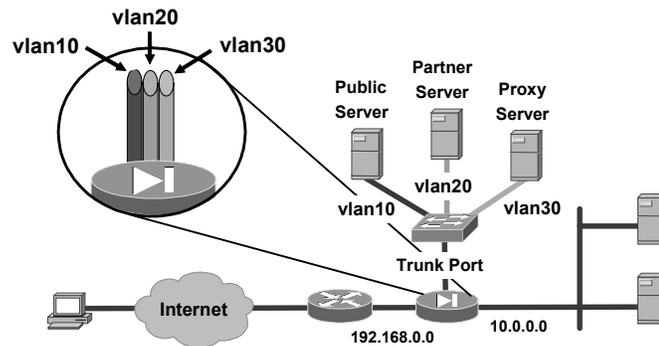
vlan20
vlan10   vlan30

Partner
Server
Public   Proxy
Server   Server

vlan10   vlan20   vlan30

Trunk Port

Internet

192.168.0.0   10.0.0.0

```
fw1(config)# interface ethernet3.1
fw1(config-subif)# vlan 10
```

SNPA v4.0—8-4

To create a logical subinterface, use the *subinterface* argument of the **interface** command in global configuration mode. To remove a subinterface, use the **no** form of this command; you cannot remove a physical interface. In subinterface configuration mode, you can assign a name, assign a VLAN, assign an IP address, and configure many other settings.

Use the **vlan** *id* command in subinterface configuration mode to assign a VLAN ID to a subinterface. The ID is an integer between 1 and 4094. Subinterfaces require a VLAN ID to pass traffic.

If you enable subinterfaces, you typically do not want the main interface to also be passing traffic, because the main interface passes untagged packets. You need to enable the main interface with the **no shutdown** command to let subinterfaces be enabled; therefore, you cannot prevent traffic from passing through the main interface with the **shutdown** command. Instead, ensure that the main interface does not pass traffic by leaving out the **nameif** command. If you want to let the main interface pass untagged packets, you can configure the **nameif** command as usual.

The syntax for the **interface** command is as follows:

```
interface {physical_interface[.subinterface] | mapped_name}
```

mapped_name	In multiple context mode, enter the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	The physical interface type and port number as typeport. A space between the type and port is optional. The physical interface types include the following: • **Ethernet** • **Gigabit Ethernet** For the PIX 500 Series Security Appliances, enter the type followed by the port number, for example, **Ethernet0 (or Ethernet 0)**. See the hardware documentation that came with your model to identify the interface type and port number.
subinterface	(Optional) An integer between 1 and 4294967293 designating a logical subinterface.

Assigning VLAN Names and Security Levels
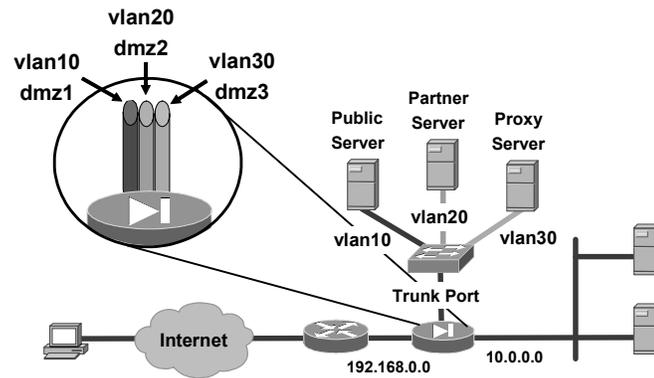
vlan20
dmz2

vlan10
dmz1

vlan30
dmz3

Public Server

Partner Server

Proxy Server

vlan10

vlan20

vlan30

Trunk Port

Internet

192.168.0.0

10.0.0.0

```
fw1(config)# interface ethernet3.1
fw1(config-subif)# vlan 10
fw1(config-subif)# nameif dmz1
fw1(config-subif)# security-level 10
```

SNPA v4.0—8-5

With the **nameif** command, the administrator defines a name for each VLAN. The interface name is used in all configuration commands on the security appliance instead of the interface type and ID (such as Gigabit Ethernet0/1), and is therefore required before traffic can pass through the interface.

To set the security level of a subinterface, use the **security-level** *number* command in subinterface configuration mode. The *number* can be any integer from 0 through 100.

In the example in the figure, vlan10 is named dmz1, with a security level of 10.

Assigning VLAN IP Addresses

Cisco.com
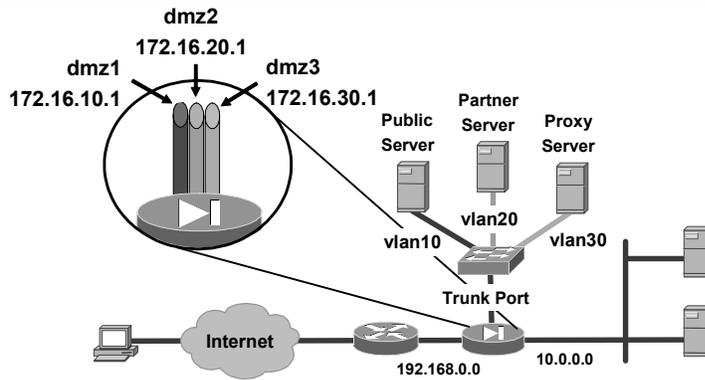
dmz2
172.16.20.1

dmz1
172.16.10.1

dmz3
172.16.30.1

Partner
Server

Public
Server

Proxy
Server

vlan20

vlan10   vlan30

Trunk Port

Internet

192.168.0.0   10.0.0.0

```
fw1(config)# interface ethernet3.1
fw1(config-subif)# vlan 10
fw1(config-subif)# nameif dmz1
fw1(config-subif)# security-level 10
fw1(config-subif)# ip address 172.16.10.1 255.255.255.0
```

SNPA v4.0—8-6

Use the **ip address** command to assign IP addresses to the VLANs. In the example in the figure, dmz1is assigned the IP address 172.16.10.1.

The syntax for the **ip address** command is as follows:

```
ip address ip_address [mask] [standby ip_address]
```

ip_address	The IP address for the interface (routed mode) or the management IP address (transparent mode).
mask	(Optional) The subnet mask for the IP address. If you do not set the mask, the security appliance uses the default mask for the IP address class.
standby *ip_address*	(Optional) The IP address for the standby unit for failover.

Example: VLAN Configuration
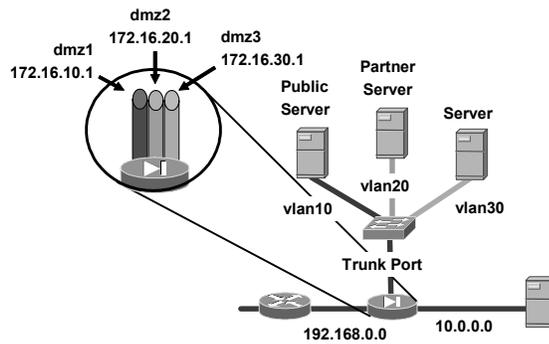
```
interface Ethernet3
   speed auto
   duplex auto
   no nameif
   no security-level
   no ip address
interface Ethernet3.1
   vlan 10
   nameif dmz1
   security-level 10
   ip address 172.16.10.1
interface Ethernet3.2
   vlan 20
   nameif dmz2
   security-level 20
   ip address 172.17.10.1
interface Ethernet3.3
   vlan 30
   nameif dmz3
   security-level 30
   ip address 172.18.10.1
```

SNPA v4.0—8-7

This figure details the configuration for creating multiple VLANs on a single physical interface. In the example, VLANs 10, 20, and 30 have been created on the appropriate subinterfaces of interface Ethernet3.

Maximum Number of Interfaces

	Restricted License		Unrestricted License	
	Physical interfaces	Virtual interfaces	Physical interfaces	Virtual interfaces
PIX Firewall 501	NA	NA	2	NA
PIX Firewall 506E	NA	NA	2	2
PIX Firewall 515E	3	10	6	25
PIX Firewall 525	6	25	10	100
PIX Firewall 535	8	50	14	150

	Physical interfaces	Virtual interfaces
ASA 5510	5	10
ASA 5520	5	25
ASA 5530	5	100

- **Maximum number of interfaces supported by Cisco PIX and ASA Security Appliance Software v7.**

SNPA v4.0—8-8

VLANs are not supported on the PIX 501, 506, and 506E Security Appliances. The number of logical interfaces that you can configure on the other Cisco security appliances varies by platform and license type.

The chart in the figure defines the maximum number of interfaces that the security appliance family supports beginning with Cisco PIX and ASA Security Appliance Software v7.0. The type of license is given across the top of the chart. The security appliances are given at the left side of the chart.

Static and Dynamic Routing

This topic explains the routing capabilities of Cisco security appliances.

Static Routes

Default Route   **Static Route**

Internet

192.168.0.1

10.0.0.102

10.0.1.11

10.0.1.4

firewall(config)#

```
route interface_name ip_address netmask gateway_ip
  [metric | tunneled]
```

- **Defines a static or default route for an interface**

```
fw1(config)# route outside 0.0.0.0 0.0.0.0 192.168.0.1 1
fw1(config)# route inside 10.0.1.0 255.255.255.0 10.0.0.102 1
```

SNPA v4.0—8-10
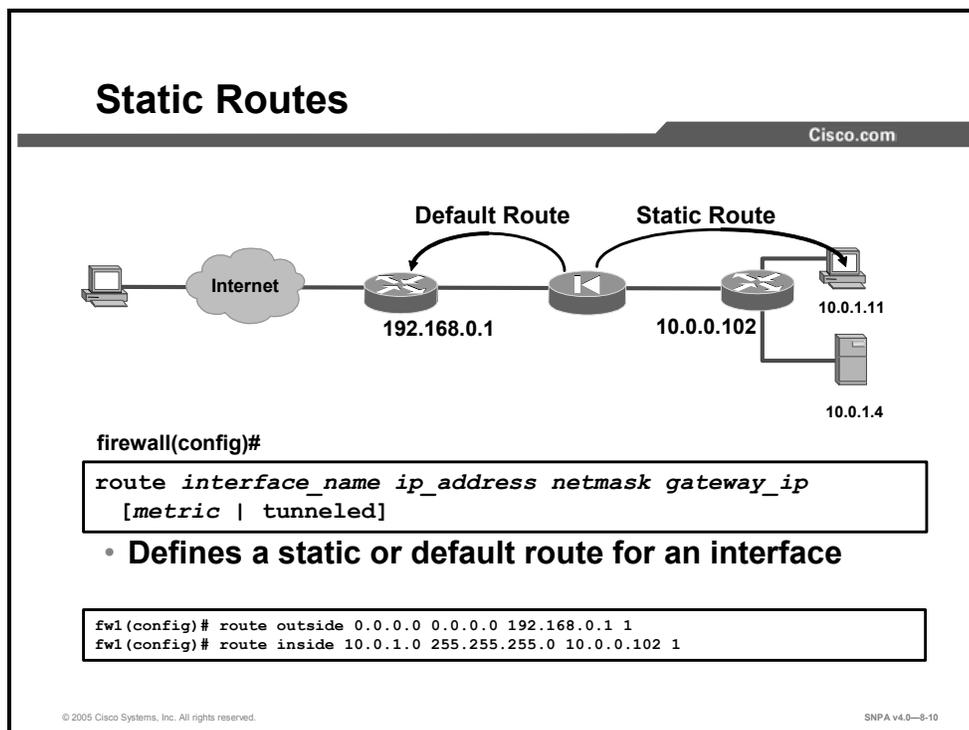
Although the security appliance is not a router, it does have certain routing capabilities. You can use the **route** command to create static routes for accessing networks outside a router on any interface. The effect of a static route is that of stating "to send a packet to the specified network, give it to this router." In the example in the figure, the security appliance sends all packets destined to the 10.1.1.0 network to the router at 10.0.0.3. All traffic for which the security appliance has no route is sent to 192.168.0.1, the gateway in the default route. To enter a default route, set the *ip_address* and *netmask* arguments to **0.0.0.0**, or the shortened form of **0**. Only one default route can be used.

All routes that are entered with the **route** command are stored in the configuration when it is saved. They can be displayed by using the **show run route** command, and you can clear most routes by using the **clear configure route** command. The only routes not removed with the **clear configure route** command are those that show the keyword **CONNECT** when you issue the **show route** command. These are routes that the security appliance automatically creates in its routing table when you enter an IP address for a security appliance interface. A route created in this manner is a route to the network directly connected to that interface.

Although the gateway argument in the **route** command usually specifies the IP address of the gateway router, the next-hop address for this route, you can also specify an interface of the security appliance. When a **route** command statement uses the IP address of a security appliance interface as the gateway IP address, the security appliance broadcasts an Address Resolution Protocol (ARP) request for the MAC address corresponding to the destination IP address in the packet instead of broadcasting the ARP request for the MAC address corresponding to the gateway IP address.

The following steps show how the security appliance handles routing in this situation:

Step 77   The security appliance receives a packet from the inside interface destined for IP address X.

Step 78   Because a default route is set to itself, the security appliance sends out an ARP for address X.

Step 79   Any Cisco router on the outside interface LAN that has a route to address X replies to the security appliance with its own MAC address as the next hop. Cisco IOS software has proxy ARP enabled by default.

Step 80   The security appliance sends the packet to router.

Step 81   The security appliance adds the entry to its ARP cache for IP address X with the MAC address being that of the router.

Dynamic RIP Routes

Cisco.com

10.0.0.1
Default Route

RIP v2

192.168.0.0   **10.0.0.0**

172.26.26.30   **Router A**

.1   .2   .1   .102   **10.0.1.11**

10.0.1.4
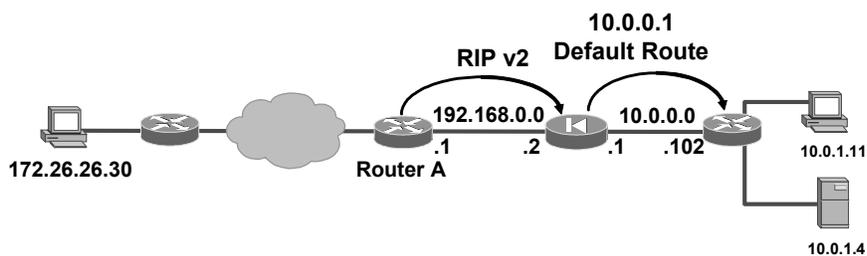
```
fw1(config)# rip outside passive version 2 authentication md5 MYKEY 2
fw1(config)# rip inside default
```

• **The security appliance accepts encrypted RIP 2 multicast updates. For example, it could learn the route to network 172.26.26.0 from router A.**

• **The appliance broadcasts IP address 10.0.0.1 as the default route for devices on the inside interface.**

SNPA v4.0—8-11

Another way to build the security appliance's routing table is by enabling RIP with the **rip** command. You can configure the security appliance to learn routes dynamically from RIP v1 or RIP v2 broadcasts. Although the security appliance uses the dynamically learned routes itself to forward traffic to the appropriate destinations, it does not propagate learned routes to other devices. The security appliance cannot pass RIP updates between interfaces. It can, however, advertise one of its interfaces as a default route.

The figure shows the security appliance learning routes from a router on its outside interface and broadcasting a default route on its inside interface. Message Digest 5 (MD5) authentication is used on the outside interface to enable the security appliance to accept the encrypted RIP updates. Both the security appliance and router A are configured with the encryption key MYKEY and its key ID value of 2.

Dynamic RIP Routes (Cont.)

Cisco.com

RIP v2

172.26.26.30   **192.168.0.0**   **10.0.0.0**   **10.0.1.0**

RIP v2 → ← **RIP v1**
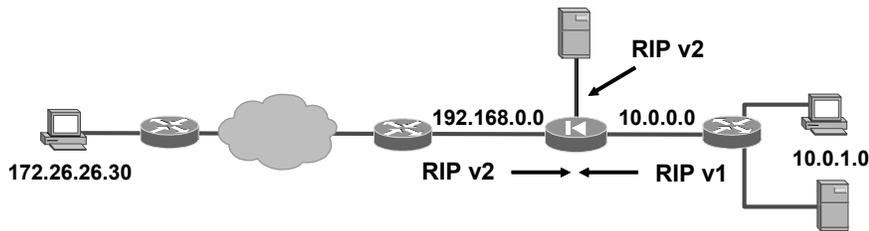
firewall(config)#

```
rip if_name default | passive [version [1 | 2]]
  [authentication [text | md5 key key_id]]
```

- **Enables IP routing table updates from received RIP broadcasts**

```
fw1(config)# rip outside passive version 2 authentication md5 MYKEY 2
fw1(config)# rip inside passive
fw1(config)# rip dmz passive version 2
```

SNPA v4.0—8-12

Use the **rip** command to configure the security appliance to learn routes dynamically from RIP v1 or RIP v2 broadcasts. When RIP v2 is configured in passive mode, the security appliance accepts RIP v2 multicast updates with an IP destination of 224.0.0.9. In the RIP v2 default mode, the security appliance transmits default route updates using an IP destination of 224.0.0.9. Configuring RIP v2 registers the multicast address 224.0.0.9 on the interface that is specified in the command so that the security appliance can accept multicast RIP v2 updates. When the RIP v2 commands for an interface are removed, the multicast address is unregistered from the interface card.

If you specify RIP v2, you can also encrypt RIP updates using MD5 encryption. Ensure that the key and key ID values are the same as those in use on any device in your network that makes RIP v2 updates.

IP routing table updates are enabled by default. Use the **no rip** command to disable the security appliance IP routing table updates on an interface. The **clear configure rip** command removes all the **rip** commands from the configuration.

Note   Static routes override dynamic routes.

The example in the figure combines RIP v1 and v2 commands that enable the following:

- Using MD5 authentication on the outside interface to encrypt the key used by the security appliance and other RIP peers, such as routers

- Broadcasting a default route on the outside interface using MD5 authentication

- Listening on the inside interface

- Listening on the demilitarized zone (DMZ) interface

The syntax for the **rip** command is as follows:

```
rip if_name default | passive [version [1 | 2]]
[authentication [text | md5 key key_id]]
```

authentication	(Optional) Enables RIP v2 authentication.
default	Broadcasts a default route on the interface.
if_name	The interface on which RIP is being enabled.
key	Key to authenticate RIP updates.
key_id	Key ID value; valid values range from 1 through 255.
md5	Uses MD5 for RIP message authentication.
passive	Enables passive RIP on the interface. The interface listens for RIP routing broadcasts and uses that information to populate the routing tables but does not broadcast routing updates.
text	Uses clear text for RIP message authentication (not recommended).
version	(Optional) Specifies the RIP version; valid values are **1** and **2**.

OSPF

This topic provides a basic explanation of the OSPF capabilities of Cisco security appliances.

Prior to Cisco PIX Security Appliance Software v6.3, Cisco security appliances supported static routing and limited dynamic routing through passive RIP. Release 6.3 introduced support for dynamic routing using the OSPF routing protocol. OSPF is widely deployed in large internetworks because of its efficient use of network bandwidth and its rapid convergence after changes in topology. Some of the OSPF-supported features of Cisco security appliances are:

■ Support for intra-area, interarea, and external (type 1 and 2) routes

■ Support for virtual links

■ Support for configuring the security appliance as a designated router, an Area Border Router (ABR), and a limited Autonomous System Boundary Router (ASBR)

■ Support for stub areas and not-so-stubby areas (NSSAs)

■ ABR type 3 link-state advertisement (LSA) filtering

■ Route redistribution

Note   OSPF routing is not supported on the Cisco PIX 501 Security Appliance. Also, OSPF and RIP cannot be enabled simultaneously on a security appliance.

Configuring OSPF

Router OSPF 1

10.0.0.0

0

Internet

OSPF

OSPF

10.0.1.0

OSPF

2.2.0.0
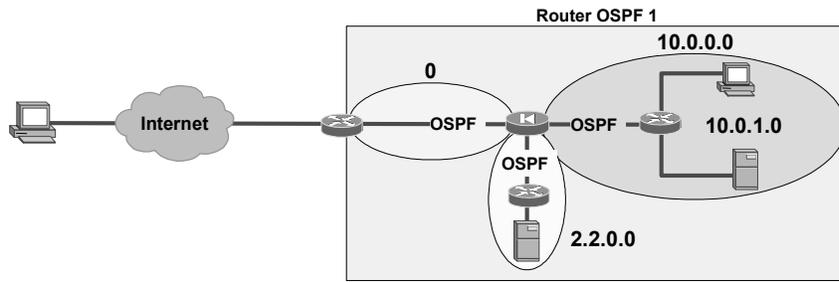
- **Enable OSPF**
- **Define interfaces on which OSPF runs**
- **Define OSPF areas**

SNPA v4.0—8-15

To configure OSPF on your security appliance, you must do the following:

- Enable OSPF.
- Define the security appliance interfaces on which OSPF runs.
- Define OSPF areas.

Enabling OSPF Routing

Cisco.com

Router OSPF 1

Internet

0

10.0.0.0

1.1.1.0

10.0.1.0

2.2.0.0

10.0.0.0
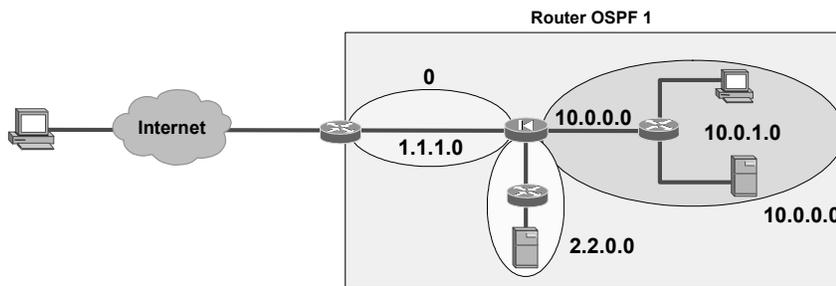
firewall(config)#

```
router ospf pid
```

- **Enables OSPF routing through the security appliance**

```
fw1(config)# router ospf 1
```

SNPA v4.0—8-16

To enable OSPF routing, use the **router ospf** command. The syntax for the **router ospf** command is as follows:

```
router ospf pid
```

pid	Internally used identification parameter for an OSPF routing process; valid values are from 1 through 65535. The process ID (PID) on one router does not need to match the OSPF PIDs on other routers.

The security appliance can be configured for one or two processes, or OSPF routing domains. If the security appliance is functioning as an ABR and it is configured for one process, the security appliance will pass type 3 LSAs between defined OSPF areas. In the example in the figure, the security appliance is configured for one OSPF process, OSPF 1.

Defining OSPF Networks
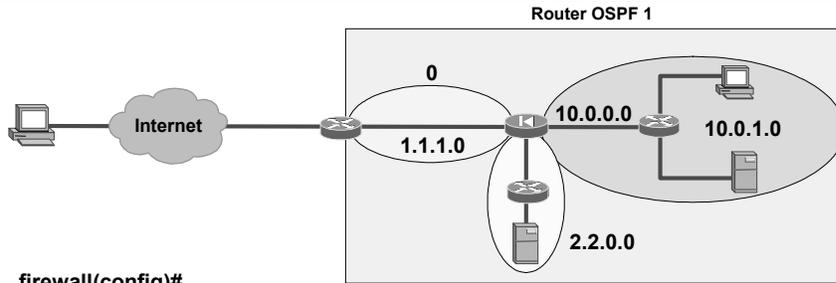
Router OSPF 1

```
firewall(config)#
```

```
network addr mask area area_id
```

- **Adds and removes interfaces to and from the OSPF routing process**

```
fw1(config)# router ospf 1
fw1(config-router)# network 1.1.1.0 255.255.255.0 area 0
fw1(config-router)# network 2.2.1.0 255.255.255.0 area 2.2.0.0
fw1(config-router)# network 10.0.0.0 255.255.255.0 area 10.0.0.0
```

SNPA v4.0—8-17

To define the interfaces on which OSPF runs and the area ID for those interfaces, use the **network area** subcommand.

The syntax for the **network area** command is as follows:

network *addr* mask area *area_id*

addr	IP address.
area *area_id*	Specifies the area that is to be associated with the OSPF address range. It can be specified in either IP address format or in decimal format. When specified in decimal format, valid values range from 0 through 4294967295.
mask	The network mask.

In the example in the figure, the three security appliance interfaces are configured for OSPF. The outside interface, network 1.1.1.0, is configured as area 0. The DMZ interface, network 2.2.1.0, is configured as network 2.2.0.0. The inside interface, network 10.0.0.0, is configured as area 10.0.0.0. Type 3 LSAs pass between the three interfaces.

OSPF: Two Processes

Router OSPF 1   Router OSPF 2

Internet

0

10.0.0.0   10.0.1.0

1.1.1.0

192.168.1.0
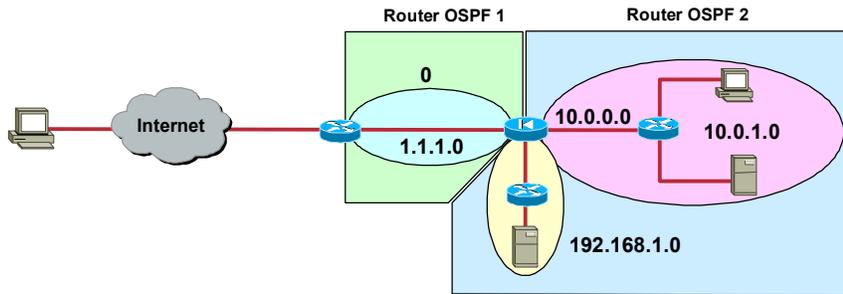
PIX Firewall OSPF two-process criteria:
- **NAT is used.**
- **OSPF is operating on public and private areas.**
- **LSA type 3 filtering is required.**

Run two OSPF processes:
- **One process is for public areas.**
- **One process is for the private areas.**

Defining a security appliance with two OSPF processes enables the security appliance to pass type 3 LSAs between areas but not between processes. In the example in the figure, there are two defined process areas. OSPF process ID 1 encompasses OSPF area 0. OSPF process ID 2 encompasses areas 10.0.0.0 and 192.168.1.0. With two OSPF processes defined, type 3 LSAs can pass between areas within a process; for example, between 192.168.1.0 and 10.0.0.0. They cannot pass between areas defined by different processes. For example, 10.0.0.0 type 3 LSAs cannot pass to area 0.

It might be advantageous to use two OSPF processes when:

- Network Address Translation (NAT) is used.

- OSPF is operating on the public and private interfaces.

- Type 3 LSA filtering is required.

A maximum of two processes can be defined for each security appliance.

Configuring Two OSPF Areas
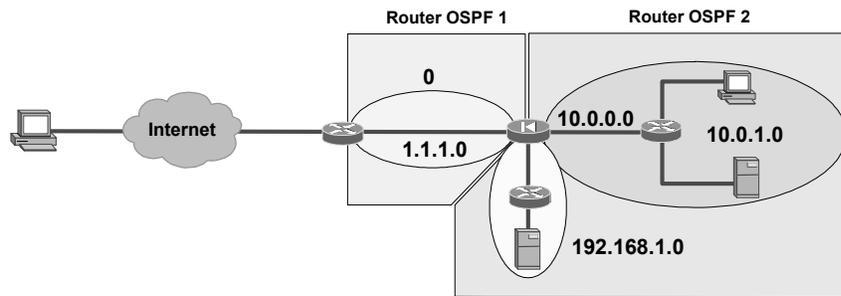
Router OSPF 1   **Router OSPF 2**

```
0
                                    10.0.0.0
Internet                                        10.0.1.0
                      1.1.1.0

                                    192.168.1.0
```

```
fw1(config)# router ospf 1
fw1(config-router)# network 1.1.1.0 255.255.255.0 area 0
fw1(config)# router ospf 2
fw1(config-router)# network 10.0.0.0 255.255.255.0 area 10.0.0.0
fw1(config-router)# network 192.168.1.0 255.255.255.0 area 192.168.1.0
```

SNPA v4.0—8-19

To configure two areas, define the router OSPF PID first. Next define the network and areas belonging to the OSPF PID. In the figure in the example, there are two OSPF PIDs, OSPF 1 and OSPF 2. OSPF 1 is defined first. Network 1.1.1.0/24 is associated with area 0.

OSPF 2 is configured next. Within OSPF 2, there are two networks, 10.0.0.0 and 192.168.1.0. Network 10.0.0.0/24 is associated with OSPF area 10.0.0.0. Network 192.168.1.0/24 is associated with area 192.168.1.0. Type 3 LSAs can pass between areas of OSPF 2. They cannot pass between OSPF 1 and OSPF 2.

Multicasting

This topic explains how to configure Cisco security appliances to allow multicast traffic.

IP Multicasting

Cisco.com

- **An IP datagram is transmitted to a set of hosts identified by a single IP destination address.**
- **Clients that wish to receive multicasts must join a multicast host group.**
- **The multicast router discovers group hosts by sending IGMP query messages.**
- **Host group members respond with IGMP reports.**
- **The security appliance supports SMR-IGMP proxying.**

© 2005 Cisco Systems, Inc. All rights reserved.   SNPA v4.0—8-21

IP multicasting is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to multiple recipients. Applications that take advantage of multicasting include video conferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news.

IP multicasting is actually the transmission of an IP datagram to a host group, a set of hosts identified by a single IP destination address. In order for this to work, hosts that wish to receive multicasts must "tune in" to the multicast by joining a multicast host group, and routers that forward multicast datagrams must know which hosts belong to which group. Routers discover this information by sending Internet Group Management Protocol (IGMP) query messages through their attached local networks. Host members of a multicast group respond to the query by sending IGMP "reports" that state which multicast group they belong to. If a host is removed from a multicast group, it sends a "leave" message to the multicast router.

In Cisco PIX Security Appliance Software v6.2 and higher and Cisco PIX and ASA Security Appliance Software v7.0 and higher, Stub Multicast Routing (SMR) is supported, which enables the security appliance to pass multicast traffic. This feature is necessary when hosts that need to receive multicast transmissions are separated from the multicast router by a security appliance. With SMR, the security appliance acts as an IGMP proxy agent. It forwards IGMP messages from hosts to the upstream multicast router, which takes responsibility for forwarding multicast datagrams from one multicast group to all other networks that have members in the group. When SMR is used, it is not necessary to construct generic routing encapsulation (GRE) tunnels to allow multicast traffic to bypass the security appliance.

Note   The GRE protocol is used for tunneling data across an IP network.

Outside Multicast Server: Configuring Outside Interface

Cisco.com

Multicast Server

Multicast Router

Outside

Multicast Group
224.0.1.50

Multicast Client
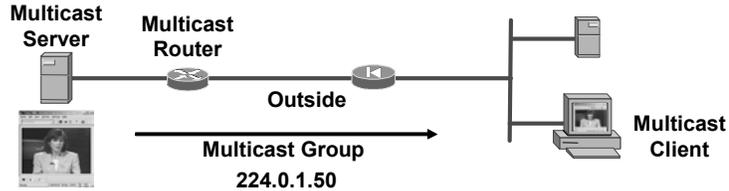
firewall(config-if)#

```
igmp access-group acl
```

- **Enables multicast support on the specified interface and places the interface in multicast promiscuous mode**
- **Applies ACL to multicast interface**

```
fw1(config)# access-list 110 permit udp any host 224.0.1.50
fw1(config)# interface ethernet0
fw1(config-if)# igmp access-group 110
```

SNPA v4.0—8-22

When hosts that need to receive a multicast transmission are separated from the multicast router by a security appliance, configure the security appliance to forward IGMP reports from the downstream hosts and to forward multicast transmissions from the upstream router. By default, IGMP processing is enabled on an interface. Complete the following steps to allow hosts to receive multicast transmissions through the security appliance on the outside interface:

Step 82 Use the **interface** command to enter the interface subcommand mode. From this prompt, you can enter the **igmp** commands for further multicast support.

Step 83 (Optional) Use the **permit** option of the **access-list** command to configure an access control list (ACL) that allows traffic to the desired Class D destination addresses. You can also use the **deny** option to deny access to transmissions from specific multicast groups. Within the ACL, the *destination-addr* argument is the Class D address of the multicast group to which you want to permit or deny multicast transmissions. If you use ACLs for this purpose, you must also use the **igmp access-group** command to apply the ACL to the currently selected interface.

The syntax for the **igmp access-group** subcommand is as follows:

```
igmp access-group acl
```

acl	Name of an IP ACL. You can specify a standard or and extended ACL. However, if you specify an extended ACL, only the destination address is matched; you should specify any for the source.

Outside Multicast Server: Configuring Inside Interface

Multicast Server **Multicast Router** **Inside**

IGMP Reports **Multicast Client**
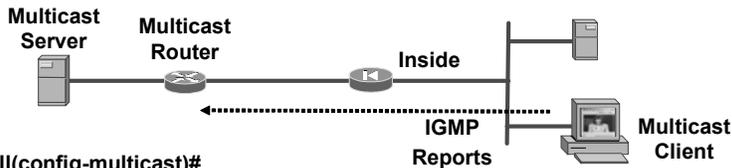
`firewall(config-multicast)#`

```
igmp forward interface if-name
```

- **Enables forwarding of IGMP reports to the multicast router on outside interface**

`firewall(config-multicast)#`

```
igmp join-group group-address
```

- **Enables security appliance to join a multicast group**

```
fw1(config)# interface ethernet1
fw1(config-if)# igmp forward interface outside
fw1(config-if)# igmp join-group 224.0.1.50
```

SNPA v4.0—8-23

Complete the following steps to allow hosts to receive multicast transmissions through the security appliance on the inside interface:

Step 84   Use the **interface** command to enter the interface subcommand mode. From this prompt, you can enter the **igmp** commands for further multicast support.

Step 85   Use the **igmp forward interface** command to enable IGMP forwarding on the security appliance. The **igmp forward interface** command enables forwarding of all IGMP host report and leave messages received by the security appliance to the specified interface. The interface specified is the security appliance interface connected to the multicast router. In the example in the figure, this is the outside interface.

Step 86   (Optional) Use the **igmp join-group** command to configure the security appliance to join a multicast group. This command configures the interface to be a statically connected member of the specified group. It allows the security appliance to act for a client that may not be able to respond via IGMP but that still requires reception. The **igmp join-group** command is applied to the downstream interface toward the receiving hosts.

A multicast group is defined by a Class D IP address. Although Internet IP multicasting uses the entire range of 224.0.0.0 through 239.255.255.255, any group address that you assign must be within the range 224.0.0.2 through 239.255.255.255. Because the address 224.0.0.0 is the base address for Internet IP multicasting, it cannot be assigned to any group. The address 224.0.0.1 is assigned to the permanent group of all IP hosts (including gateways). This is used to address all multicast hosts on the directly connected network. There is no multicast address (or any other IP address) for all hosts on the total Internet.

The syntax for the **igmp** subcommands discussed above is as follows:

```
igmp forward interface if-name
igmp join-group group-address
```

if-name	Logical name of the interface.
group-address	IP address of the multicast group.

Outside Multicast Server Example: Inside Receiving Hosts

1. Host 10.0.0.11 sends an IGMP report:
   Source 10.0.0.11
   Destination 224.0.1.50
   IGMP group 224.0.1.50
2. The security appliance accepts the packet, and IGMP places the inside interface on the output list for the group.
3. The security appliance forwards the IGMP packet to the multicast router:
   Source 172.16.0.1
   Destination 224.0.1.50
   IGMP group 224.0.1.50
4. The router places the input interface on the output list for the group.
5. Packets from the multicast server arrive at the router, which forwards them to the necessary interfaces.
6. The security appliance accepts the packets and forwards them to the interfaces for the group.

172.16.0.1

Multicast Router

Multicast Server

Multicast Group 224.0.1.50

IGMP Reports

Multicast Client 10.0.0.11
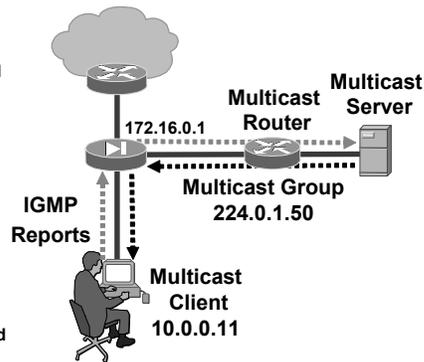
```
fw1(config)# access-list 120 permit udp any host 224.0.1.50
fw1(config)# interface ethernet2
fw1(config-if)# igmp access-group 120
fw1(config)# interface ethernet1
fw1(config-if)# igmp forward interface dmz
```

SNPA v4.0—8-24

The figure shows the use of the **interface** command with corresponding **igmp** subcommands. Multicasting is permitted on the DMZ and inside interfaces. The **igmp forward interface** command enables the security appliance to forward IGMP reports from inside hosts to the multicast router on its DMZ interface.

In the example in the figure, host 10.0.0.11 joins multicast group 224.0.1.50. The security appliance enables host 10.0.0.11 to receive multicasts from the multicast server.

Configuring Other IGMP Options

firewall(config-if)#

```
igmp version {1 | 2}
```

- **Sets the version of IGMP to be used**

firewall(config-if)#

```
igmp query-interval seconds
```

- **Configures the frequency at which IGMP query messages are sent by the interface**

firewall(config-if)#

```
igmp query-max-response-time seconds
```

- **Sets the maximum query response time (for IGMP 2 only)**

```
fw1(config)# interface ethernet0
fw1(config-if)# igmp version 2
fw1(config-if)# igmp query-interval 120
fw1(config-if)# igmp query-max-response-time 25
```

SNPA v4.0—8-25

There are some other IGMP options that can be set by an administrator. The administrator can choose an IGMP version and configure the IGMP timers with the **igmp query-interval** and **igmp query-max-response-time** commands. To specify the version of IGMP, use the **igmp version** command. This configures which version of IGMP is used on the subnet that is represented by the specified interface. The default is version 2.

IGMP v2 offers bandwidth-conserving features that are not available in version 1. The Leave Group message is one of these features. This message reduces the bandwidth waste between the time the last host in a subnet drops membership and the time the router times out for its queries and decides there are no more members present for that group.

For further information on the differences between IGMP v1 and IGMP v2, see RFC 2236.

Use the **igmp query-interval** command to configure the frequency at which IGMP query messages are sent by the interface. The default is 60 seconds. The permitted range of values is from 1 through 65535. Use the command **no igmp query-interval** to set the query interval back to the default.

The **igmp query-max-response-time** command specifies the maximum query response time and is available only with IGMP v2. The default is 10 seconds. The permitted range of values is from 1 to 25. Use the command **no igmp query-max-response-time** to set the query response time back to the default.

The syntax for these **igmp** commands is as follows:

```
igmp version {1 | 2}
igmp query-interval seconds
igmp query-max-response-time seconds
```

query-interval	The query response time interval.
query-max-response-time	The maximum query response time interval.
seconds	The number of seconds to wait.

Protocol Independent Multicast Sparse Mode Overview
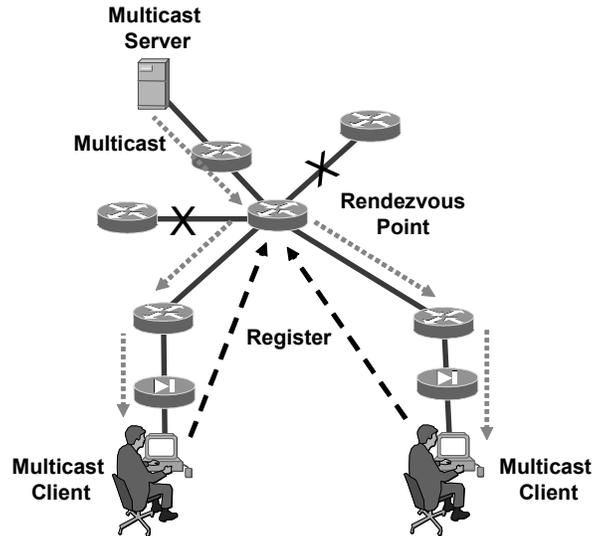
SNPA v4.0—8-26

In Protocol Independent Multicast sparse mode (PIM SM), each data stream goes to a relatively small number of segments in the campus network. Instead of flooding the network to determine the status of multicast members, PIM SM defines a rendezvous point. The rendezvous point keeps track of multicast groups. When a user wants to send data, the user first sends to the rendezvous point. When a user wants to receive data, the user registers with the rendezvous point. After the data stream begins to flow from sender to rendezvous point to receiver, the routers in the path will optimize the path automatically to remove any unnecessary hops. PIM SM assumes that no hosts want the multicast traffic unless they specifically ask for it. Sparse-mode protocols begin with an empty distribution tree and add branches only as the result of explicit requests to join the distribution.

PIM SM is optimized for environments in which there are many multipoint data streams. PIM SM is most useful when:

- There are few receivers in a group
- The type of traffic is intermittent

Configuring PIM

Multicast Server

Rendezvous Point
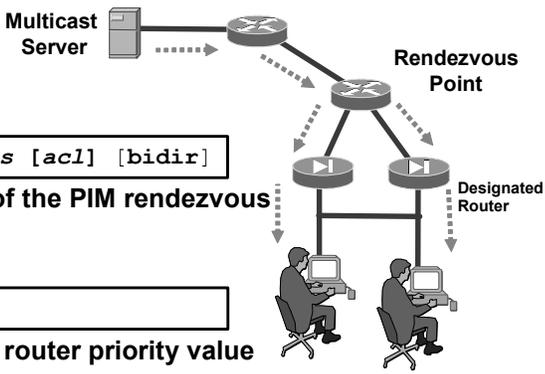
Designated Router

firewall(config)#

```
pim rp-address ip_address [acl] [bidir]
```

- **Configures the address of the PIM rendezvous point.**

firewall(config-if)#

```
pim dr-priority num
```

- **Changes the designated router priority value**

```
fw1(config)# multicast-routing
fw1(config)# pim rp-address 192.168.10.1
fw1(config)# interface ethernet1
fw1(config-if)# pim dr-priority 5
```

SNPA v4.0—8-27

Devices use PIM to maintain forwarding tables for forwarding multicast packets. To enable IP multicast routing on the security appliance, use the **multicast routing** command in global configuration mode. When you enable multicast routing on the security appliance, PIM is automatically enabled on all interfaces.

All routers within a common PIM SM domain require knowledge of the well-known PIM rendezvous point address. Rendezvous points are used by senders to a multicast group to announce their existence. The first-hop routers send PIM register messages to the rendezvous point on behalf of a host sending packets to the group. Rendezvous points are used by receivers of multicast packets to learn about new senders. The last-hop routers send PIM join and prune messages to the rendezvous point to inform it about group membership.

To configure the address of the PIM rendezvous point, enter this command:

> hostname(config)# **pim rp-address** *ip_address* [*acl*] [**bidir**]

The *ip_address* argument is the unicast IP address of the router to be a PIM RP. The *acl* argument is the name or number of an ACL that defines which multicast groups the rendezvous point should be used with. Optionally, if **bidir** is entered, it indicates that the specified multicast groups are to operate in bidirectional mode. If the command is configured without this option, the specified groups operate in PIM SM.

Note   The security appliance does not support automatic rendezvous point; you must use the **pim rp-address** command to specify the rendezvous point address.

When there is more than one multicast security appliance on a network segment, the designated router is responsible for sending PIM register, join, and prune messages to the rendezvous point. There is an election process to select the designated router based on designated router priority. If multiple devices have the same designated router priority, then the device with the highest IP address becomes the designated router. By default, the security appliance has a designated router priority of 1. To change the priority, use the **pim dr-priority** command in the interface subcommand mode. The *num* argument can be any number from 1 through 4294967294.

Viewing SMR Configuration

Cisco.com

firewall #

```
show mfib [active count interface reserved status
  summary verbose]
```

- **Displays IP MFIB**

firewall#

```
show mrib [client route (route summary)]
```

- **Displays MRIB**

firewall#

```
show mroute
```

- **Displays multicast routes**

SNPA v4.0—8-28

The following commands can be used to view the current multicast and IGMP configuration:

- **show mfib**: Displays the Multicast Forwarding Information Base (MFIB) in terms of forwarding entries and interfaces

- **show mfib active**: Displays active multicast sources

- **show mfib count**: Displays MFIB route and packet count data

- **show mfib interface**: Displays packet statistics for interfaces that are related to the MFIB process

- **show mfib reserved**: Displays reserved groups

- **show mfib status**: Displays the general MFIB configuration and operational status

- **show mfib summary**: Displays summary information about the number of MFIB entries and interfaces

- **show mfib detail**: Displays detail information about the forwarding entries and interfaces

- **show mrib client**: Displays information about the Multicast Routing Information Base (MRIB) client connections

- **show mrib route**: Displays entries in the MRIB table

- **show mrib route summary**: Displays a summary of the MRIB table entries

- **show mroute**: Displays multicast routes

Debugging SMR Configuration

```
firewall#
```
```
debug igmp
```

- **Enables debugging for IGMP events**

```
firewall#
```
```
debug mfib
```

- **Enable debugging for MFIB**

```
firewall#
```
```
debug mrib
```

- **Enable debugging for MRIB**

SNPA v4.0—8-29

You can use the following commands for debugging your SMR configuration:

- **debug igmp**: Enables or disables debugging for IGMP events
- **debug mfib**: Enables or disables debugging for the MFIB
- **debug mrib**: Enables or disables debugging for the MRIB

Each of these commands can be removed by using its **no** form.

Summary

This topic summarizes the information you learned in this lesson.

Summary

- **Cisco PIX Firewall 500 Series Security Appliances (except 501, 506, and 506E) and Cisco ASA 5500 Series Adaptive Security Appliances support 802.1 VLANs.**
- **You can add static routes to a security appliance to enable access to remote networks.**
- **Security appliances can be configured to listen for RIP 1 or RIP 2 routing broadcasts.**
- **Security appliances cannot pass RIP updates between interfaces.**
- **RIP 2 updates use multicast address 224.0.0.9 and support MD5 authentication for secure routing updates.**
- **Security appliances support one or two OSPF routing domains.**
- **Security appliances support OSPF intra-area and interarea routing.**
- **Security appliances support ABR type 3 LSA filtering.**
- **Security appliances supports Stub Multicast Routing, which enables passing multicast traffic between transmission sources and receiving hosts on different interfaces.**

SNPA v4.0—8-30

Lesson 9

Modular Policy Framework

Overview

This lesson introduces Cisco Modular Policy Framework. It explains how to configure a modular policy, how to configure a class map, how to associate a policy with the newly created class map, and how to apply the policy to an interface or globally.

Objectives

Upon completion of this lesson, you will be able to describe and configure a security appliance modular policy. This includes being able to meet these objectives:

- Explain the Cisco Modular Policy Framework feature for security appliances
- Configure a class map
- Configure a policy map
- Configure a service policy

Modular Policy Overview

This topic discusses what Cisco Modular Policy Framework is and how it works.

Modular Policy Framework Overview

Cisco.com

System Engineers

Internet

Headquarters

Executives

Internet

384 K   384 K

Site C   Site B

Cisco Modular Policy Framework provides greater granularity and more flexibility when configuring network policies.

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

SNPA v4.0—9-3

There is a growing need to provide greater granularity and flexibility in configuring network policies, for example, the ability to identify and prioritize voice traffic, the ability to rate-limit groups of remote access virtual private network (VPN) connections, the ability to perform deep packet inspection on specific flows of traffic, and the ability to set connection values. Cisco PIX and ASA Security Appliance Software v7.0 provides this functionality with the introduction of Cisco Modular Policy Framework, a framework in which users have the ability to define traffic classes at the desired granularity and apply actions (policies) to them.

Modular Policy

Cisco.com

System Engineers

Internet

Headquarters

Executives

Internet

384 K   384 K

Site C

Site B
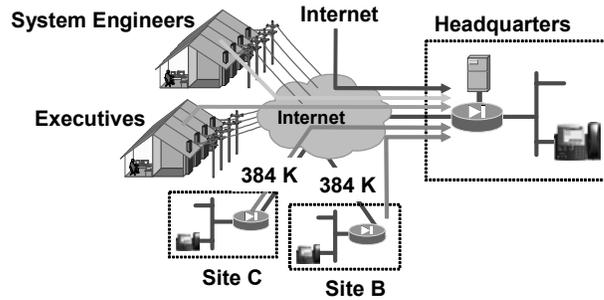
Modular policy provides greater granularity and more flexibility

Class Map		Policy Map		Service Policy
Traffic flow		Outside policy map		Interface and Global
Internet	→	Inspect		
SE	→	IPS		Outside
EXEC		Police		
s2s_voice	→	Priority		
Default inspection	→	Global policy	→	Global
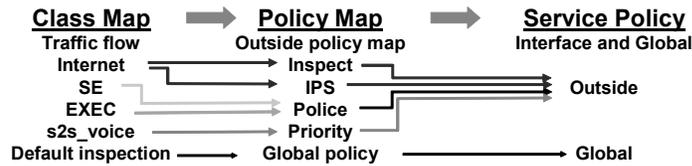
© 2005 Cisco Systems, Inc. All rights reserved.

SNPA v4.0—9-4

Cisco Modular Policy Framework is configured using three main commands:

- **class-map**: Used to identify a traffic flow. A traffic flow is a set of traffic that is identifiable by its packet content. The example in the figure shows voice traffic between site B and headquarters (s2s_voice) and remote access VPN to headquarters for the system engineers (SE) and executives (EXEC) .

- **policy-map**: Used to associate one or more actions with a class of traffic. For example, all voice traffic between site B and headquarters is provided with low latency queuing (LLQ).

- **service-policy**: Used to enable a set of policies on an interface. For example, the voice priority queuing policy is applied to the outside interface.

In the example in the figure, a network administrator identified five traffic flows: Internet traffic; system engineer remote VPN traffic; executive remote VPN traffic; and two site-to-site VPN tunnels, to site B and site C, with voice. After the traffic flows are identified, security policies are associated to each flow. The policy for traffic from the Internet is to perform deep packet inspection and inline intrusion prevention. The administrator will police the amount of bandwidth used by the system engineer and executive remote VPN traffic. For site-to-site traffic over a VPN, all voice connection traffic is given high-priority queuing. The last class is the default inspection class. All traffic is subject to the default inspection policy.

After the classes and policies are defined, policies are assigned to a specific interface or assigned globally. In the example in the figure, the global_policy policy map is assigned globally. The outside_policy policy map is assigned to the outside interface.

Configuring a Class Map

This topic explains how to configure a class map.

Assigning a Class Map Name

Cisco.com

To configure a class map:
- Name a class
- Define matching attributes

System Engineers Internet Headquarters

Executives

Site C   Site B

- **Assign a name to the class of traffic**

```
pix1(config)# class-map se
pix1(config)# class-map exec
pix1(config)# class-map s2s_voice
pix1(config)# class-map internet
```

SNPA v4.0—9-6

The **class-map** command is used to classify a set of traffic with which security actions may be associated. Configuring a class map is a two-step process, naming the class of traffic and defining the attributes of the traffic. A name is assigned to each individual class of traffic. In the example in the figure, four traffic classes are named. The **class-map se** command identifies the remote VPN traffic to the system engineers. The **class-map s2s_voice** command identifies the site-to-site VPN traffic. The **class-map internet** command identifies traffic from the Internet.

The syntax of the **class-map** commands is as follows:

```
class-map class_map_name
```

Defining a Class of Traffic

To configure a class map:
- **Name a class**
- **Define matching attributes**

Define a class of traffic by matching:
- access-list—**ACL**
- any—**Any packet**
- default-inspection-traffic—**Match** inspection **commands**
- dscp—**Match IP differentiated services code point**
- flow—**Match the destination IP address**
- port—**Match TCP and UDP port(s)**
- precedence—**Match IP precedence**
- rtp—**Match RTP port numbers**
- tunnel-group—**Match a VPN tunnel group**
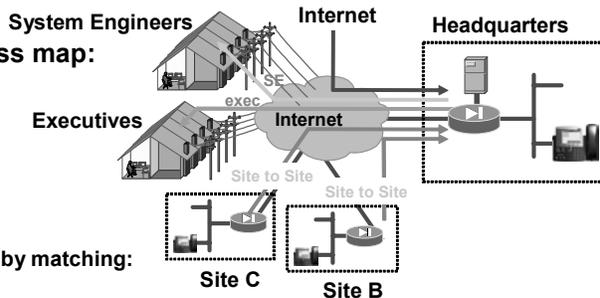
SNPA v4.0—9-7

After a class of traffic is named, the characteristics of the traffic flow are identified. To be considered part of a named class, a traffic flow must match a defined set of attributes. There are various types of matchable criteria in a class map.

The following is the class matching criteria:

- **access-list**—Keyword specifies to match an entry in an access-list.

- **any**—Keyword specifies that all traffic is to be matched. **match any** is used in the 'inspection_default' class-map; it means match any packet.

- **dscp**—Keyword specifies to match the Internet Engineering Task Force (IETF)-defined differentiated services code point (DSCP) value in the IP header. This criterion allows the user to define classes based on the DSCP values that are defined within the type of service (ToS) byte in the IP header.

- **flow**—Keyword pair specifies to match the destination IP address (within a tunnel group). This **match** command must be used in conjunction with the **match tunnel-group** command.

- **port**—Keyword specifies to match traffic using the TCP or User Datagram Protocol (UDP) destination port.

- **precedence**—Keyword specifies to match the precedence value represented by the ToS byte in the IP header. This criterion allows the user to define classes based on the precedence defined within the ToS byte in the IP header.

- **rtp**—Keyword specifies to match Real-Time Transport Protocol (RTP) destination port. This criterion allows the user to match on a UDP port number within the specified range. The allowed range is targeted at capturing applications that are likely to be using RTP. The packet matches the defined class only if the UDP port falls within the specified range, inclusive, and the port number is an even number.

- **tunnel-group**—Keyword specifies to match tunnel traffic.

The syntax of the **class-map** commands is as follows:

```
class-map <classmap_name>
        description <text>
        match any
        match access-list <acl_name>
        match port  tcp | udp {eq <n> | range <n1> <n2>}
        match precedence <precedence_value>
        match dscp <dscp_value>
        match rtp <starting_port> <range>
        match tunnel-group <tunnel_group_id>
        match flow ip destination-address
        match default-inspection-traffic
```

classmap_name	Name for the class map; up to 40 characters.	
	"inspection_default" is a reserved name for default class. It always exists and it can't be configured or removed via CLI. When used in a policy map, a default class means "all other traffic." The actual syntax of a default class is:	
	class-map *inspection_default*	
	match any	
	The name space for a class map is local to a security context. The same name may be used in different security contexts.	
	The maximum number of class maps per security context is 255.	
description	A subcommand that is used to specify a description for the class map.	
<text>	The description; up to 200 characters are allowed.	
match	A subcommand that is used to specify a match criterion.	
access-list	Keyword that specifies that an ACL is to be used as a match criterion. When a packet matches no entry in an ACL, the match result is a no-match. When a packet matches an entry in an ACL and it is a "permit" entry, the match result is a match. If it is a "deny" entry, the match result is a no-match.	
<acl_name>	Name of the ACL to be used as a match criteria.	
any	Keyword that specifies that all traffic is to be matched. **match any** is used in the inspection_default class map.	
none	Keyword that specifies that no traffic will be matched. When a class map is created with no **match** command in the class map, a **match none** is automatically created in the class map. Note that **match none** cannot be configured.	
port	Keyword that specifies to match traffic using the TCP or UDP destination port.	
tcp	Keyword that specifies to match traffic using a TCP destination port.	
udp	Keyword that specifies to match traffic using a UDP destination port.	
<port_name> | *<n>*	Specifies a port name, such as **HTTP**, or a port number (from 1 through-65535.	
precedence	Keyword that specifies to match the precedence value represented by the ToS byte in the IP header.	
precedence_value	Specifies the precedence value (0–7).	
dscp	Keyword that specifies to match the IETF-defined DSCP value in the IP header.	
dscp_value	Specifies the DSCP value (0–63).	
rtp	Keyword that specifies to match RTP ports (even UDP port numbers between *starting_port* and s*tarting_port+range*).	
starting_port	Specifies the lower bound of UDP destination port.	
range	Specifies the range of RTP ports.	
default-inspection-traffic	Keyword that specifies to match default traffic for individual **inspect** commands. Following are the rules of using this match criteria:	
	This match applies only to the **inspect** command as such; when the class map that contains this **match** command is used in a policy map, the class map cannot be associated with any action command other than the **inspect** command.	
	The matched traffic depends on the individual **inspect** command. See the following table for what **default-inspection-traffic** means to each	

inspect command.

This match can be used in conjunction with one other **match** command, typically an ACL in the form of **permit ip** *src-ip dst-ip.* The two **match** commands are merged to produce match rules for **inspect** commands. The merge rule is to use the protocol and port information from the **match default-inspect-traffic** command and use the nonprotocol and nonport information (such as IP addresses) from the other **match** command. So any protocol or port information in the other **match** command is ignored with respect to **inspect** commands. For example, in this configuration, port 65535 is ignored.

> **match default-inspection-traffic**
> **match port** *65535*

> or

> **access-list foo permit ip host** *192.168.1.1 any* **eq** *65535*

> **match default-inspection-traffic**
> **match access-list** *foo*

default traffic for individual inspection:

Protocol Name	Protocol	Source Port	Destination Port
ctiqbe	tcp	N/A	2748
dns	udp	53	53
ftp	tcp	N/A	21
gtp	udp	2123,3386	2123,3386
h323 h225	tcp	N/A	1720
h323 ras	udp	N/A	1718-1719
http	tcp	N/A	80
icmp	icmp	N/A	N/A
ils	tcp	N/A	389
mgcp	udp	2427,2727	2427,2727
netbios	udp	137-138	N/A
rpc	udp	111	111
rsh	tcp	N/A	514
rtsp	tcp	N/A	554
sip	tcp,udp	N/A	5060
skinny	tcp	N/A	2000
smtp	tcp	N/A	25
sqlnet	tcp	N/A	1521
tftp	udp	N/A	69
xdmcp	udp	177	177

tunnel-group	Keyword that specifies to match tunnel traffic.

<tunnel_group>	Specifies a configured tunnel-group.
flow ip	Keyword pair that specifies to match destination IP address within a flow. This **match** command must be used in conjunction with the **match tunnel-group** command.
<destination-address>	Destination address.
classmap_name	Name for the class map; up to 40 characters.
	"inspection_default" is a reserved name for default class. It always exists, and it can't be configured or removed via CLI. When used in a policy map, a default class means "all other traffic." The actual syntax of a default class is:
	class-map *inspection_default*
	match any
	The name space for the class map is local to a security context. So the same name may be used in different security contexts.
	The maximum number of class maps per security context is 255.
description	A subcommand that is used to specify a description for the class map.
<text>	Text for the description; up to 200 characters are allowed.

Defining Class Match Criteria

To configure a class map:
- **Name a class**
- **Define matching attributes**

System Engineers • Internet • Headquarters • SE • exec • Executives • Internet • Site to Site • Site to Site • Site C • Site B
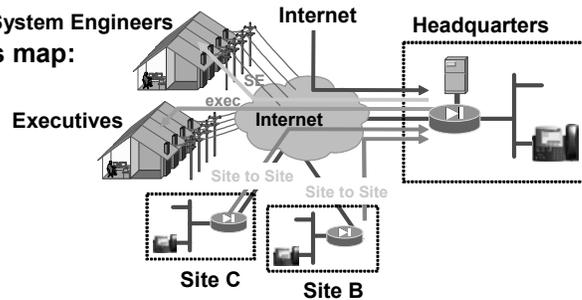
- **Define a class of traffic identified by a class map name**

```
pix1(config)# class-map se
pix1(config-cmap)# match tunnel-group se
pix1(config-cmap)# match flow ip destination-address
pix1(config)# class-map s2s_voice
pix1(config-cmap)# match tunnel-group site_c
pix1(config-cmap)# match dscp cs5
```

SNPA v4.0—9-8

You may want to police the traffic of remote access users. You also may want to route VPN site-to-site voice traffic through the priority queue. The administrator uses the **class-map** command to identify the traffic flows. In the example in the figure, the administrator defined two class maps, se and s2s_voice. The matching criteria for the remote access VPN traffic is the se tunnel group and the flow IP destination address. The security application identifies as members of the se class map any exiting traffic that both matches the system engineers remote access users tunnel group and has the destination address of system engineers remote access users. The security appliance identifies as a member of the s2s_voice class map any exiting traffic that both matches the site C tunnel group and has a DSCP of 5. Multiple **match** commands per class map are not supported except for **match tunnel-group** or **default-inspect-traffic** commands.

show run class-map Command

System Engineers **Internet** **Headquarters**

SE

exec

Executives **Internet**

Site to Site   Site to Site

Site C   **Site B**
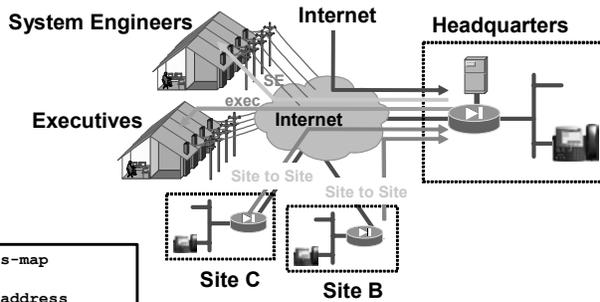
```
pix1(config)# show run class-map
class-map se
 match flow ip destination-address
 match tunnel-group se
class-map exec
 match flow ip destination-address
 match tunnel-group exec
class-map internet
 match access-list internet
class-map inspection_default
 match default-inspection-traffic
class-map s2s_voice
 match dscp cs5
 match tunnel-group site_c
```

SNPA v4.0—9-9

You can use the **show run class-map** command to view the class map configuration. You can use the **show** command to view each of the configured class maps with their matching criteria.

Configuring a Policy Map

This topic explains how to configure a policy map.

Policy Map Overview

Cisco.com

To configure Policy map:
- **Name a policy map**
- **Identify a class**
- **Associate action(s) with the class**

System Engineers · Internet · Headquarters · SE · exec · Executives · Internet · Site to Site · Site to Site · Site C · Site B

Class Name	+	Policy	=	Policy Map
Internet		IPS		Outside
SE		Inspect		
EXEC		Police		
s2s_voice		Priority		
Default inspection	+	Inspect	=	Global

SNPA v4.0—9-11

A **policy-map** command is used to configure various policies. A policy consists of a **class** command and its associated actions. The security appliance supports one policy per interface and one global policy. Each policy map can support multiple classes and policy actions. In the example in the figure, there are two policy maps, the outside_policy policy map and the global_policy policy map. The outside_policy policy map supports four class maps: Internet, SE, EXEC, and s2s_voice. IPS, Inspect, Police, and Priority actions are associated with classes. The global_policy policy map supports default inspect criteria for all traffic.

Assigning a Policy Map Name

Cisco.com

To configure Policy map:
- **Name a policy map**
- **Identify a class**
- **Associate action(s) with the class**

System Engineers

Internet

Headquarters

SE exec

Executives

Internet

Site to Site

Site to Site

Site C

Site B

- **Assign a name to the policy map**
- **Assign one or more classes to the policy map**

```
pix1(config)# policy-map outside_policy
pix1(config-pmap)# class internet
pix1(config-pmap-c)# ?
```

SNPA v4.0—9-12

Defining a **policy-map** is a three-step process: naming the policy, identifying a class of traffic covered by this policy, and associating one or more actions with each traffic flow. The first step is to name the policy maps. In the example in the figure, there are two policy maps, the outside_policy policy map and the global_policy policy map.

The next step is to identify which traffic flow classes are specified in a policy map. Each traffic flow is identified by a class map name. In the example in the figure, the outside_policy policy map is identified, and Internet class traffic flow is assigned to it.

The syntax of the **policy-map** commands is as follows:

```
policy-map <policymap_name>
            description <text>
            class <classmap_name>
```

policymap_name	Name for the policy map; up to 40 characters. The name space for a policy map is local to a security context, so the same name can be used in different security contexts. The maximum number of policy maps is 64.
Description	A subcommand that is used to specify a description for the policy map.
text	Text for the description; up to 200 characters are allowed.
class	A subcommand that is used to specify a class map for traffic classification. By default, **class inspection_default** always exists at the end of a policy map. At most, 63 **class** commands can be configured in a policy map.
classmap-name	Name of the class map. When **inspection_default** is specified, a packet that does not match any class of an action in the policy map will match the inspection_default class.

Defining a Policy for the Class

- **Define policy actions associated with one or more classes of traffic**

```
pix1(config)# policy-map outside_policy
pix1(config-pmap)# class internet
pix1(config-pmap-c)# ?

MPC policy-map class configuration commands:
  exit      Exit from MPC class action configuration mode
  help      Help for MPC policy-map configuration commands
  IPS       Intrusion Protection services
  inspect   Protocol inspection services
  no        Negate or set default values of a command
  police    Police
  priority  Strict scheduling priority for this class
  set       Set QoS values or connection values
```

SNPA v4.0—9-13

The last step in configuring a policy map is to associate action(s) with specific traffic flows within a policy map. A policy map name is defined, outside. The Internet class of traffic is identified. You must next associate action(s) with this traffic flow. The policy action options are to forward the traffic flow to the intrusion protection services, perform specified protocol inspection(s), police the bandwidth used by the specified flow, direct the flow to the low latency queue, and set connection parameters on the flows. Traffic classes for police and priority features are applied unidirectionally in the transmit direction. IPS, inspect, and set are applied bidirectionally. You can associate multiple classes within a policy map.

The syntax of the **policy-map** commands is as follows:

```
policy-map <policymap_name>
        description <text>
        class <classmap_name>
        set connection random-seq# enable | disable
        set connection {conn-max | embryonic-conn-max | } <n>
        set connection timeout tcp hh[:mm:ss] embryonic
        hh[:mm:ss] half-closed hh[:mm:ss]
        inspect {ctiqbe | dns [<max_length>] | esmtp |
                ftp [strict] [<ftp_map>] | gtp [<gtp_map>] |
                http [<http_map>] | h323 {h225 | ras} |
                icmp | icmp error | ils | mgcp [<mgcp_map>] |
                netbios | pptp | rpc | rsh | rtsp | sip [udp] |
                skinny | snmp [<snmp_map>] | sqlnet | tftp |
            xdmcp}
        IPS {inline | promiscuous} {fail-open | fail-close}
        priority
        police
```

inspect	Protocol inspection service
ips	Intrusion protection services
police	Rate-limit traffic for this class
priority	Strict scheduling priority for this class
set connection	Sets connection values

Police Policy Overview
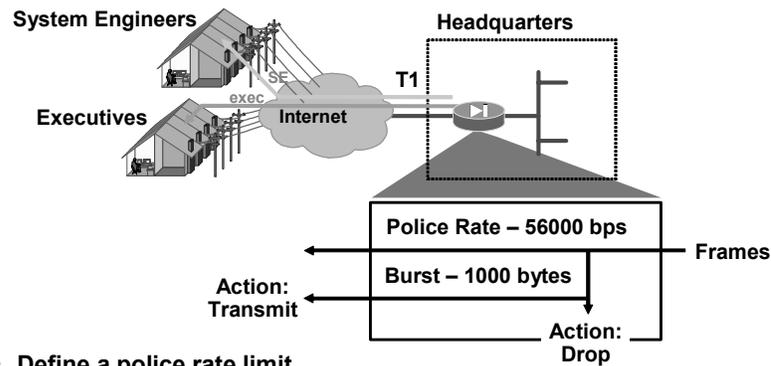
SNPA v4.0—9-14

Bandwidth policing sets a maximum transmit limit, a cap, on the rate of tunneled and nontunneled traffic. The police rate is the maximum transmit limit on the rate of sustained tunneled traffic. The security appliance transmits traffic below this police rate. Because traffic is bursty, some flexibility is built into policing. The burst size indicates the maximum size of an instantaneous burst of bytes allowed before traffic is capped to get it back to the policing rate. You can define the actions to be taken by the security appliance when the traffic exceeds the police rate but conforms to the burst size or when the traffic exceeds both the police rate and the burst size. For both the conforming and exceeding burst scenarios, you can choose to transmit or drop the bursting packets. For example, the headquarters security appliance will transfer data up to a sustained rate of 56 Kbps to the system engineers. If the security appliance experiences a transmission burst of packets, for example, up to 1000 bytes to a member of the se class of traffic, the security appliance will transmit the packets. If the burst exceeds the 1000-byte limit, the security appliance will drop the offending packets.

Example: Police Policy

Cisco.com

System Engineers

Headquarters

SE

exec

T1

Internet

Executives

Police Rate – 56000 bps

Frames

Conform:
Transmit

Burst – 1000 bytes

Exceed
(Burst Size):
Drop
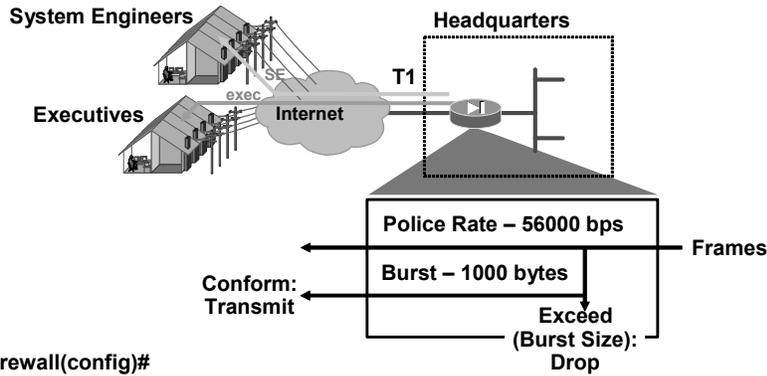
firewall(config)#

police *conform-rate conform-burst* | **conform-action {drop | transmit}** |
exceed-action {drop | transmit}}

```
pix1(config)# policy-map outside_policy
pix1(config-pmap)# class se
pix1(config-pmap-c)# police 56000 1000 conform-action transmit exceed-
action drop
```

SNPA v4.0—9-15

To configure the police action, you must configure four items: the police rate limit, the burst size, the conform action, and the exceed action. In the example in the figure, the police policy action is applied to the se class of packets. The maximum sustained transmission is 56 Kbps, and the burst size is 1000 bytes. If the traffic conforms to the rate limit and doesn't exceed the burst size, the security appliance transmits the packet. If the burst rate exceeds the rate limit and the burst size, the security appliance is configured to drop the offending traffic. This action, when enabled, is unidirectional.

The syntax of the **police** command is as follows:

```
police conform-rate conform-burst | conform-action {drop |
transmit} | exceed-action {drop | transmit}}
```

conform-action	The action to take when the rate is less than the *conform-burst* value.
conform-burst	A value from 1000 through 512000000 that specifies the maximum number of instantaneous bytes allowed in a sustained burst before throttling to the conforming rate value.
conform-rate	The rate limit for this traffic flow; a value from 8000 through 2000000000 that specifies the maximum speed (bits per second) that is allowed.
drop	Drops the packet.
exceed-action	The action to take when the rate is between the *conform-rate* value and the *conform-burst* value.
drop	Drops the packet.
transmit	Transmits the packet.

Intrusion Prevention Policy Overview

Cisco.com

Internet

Headquarters

Internet

IPS
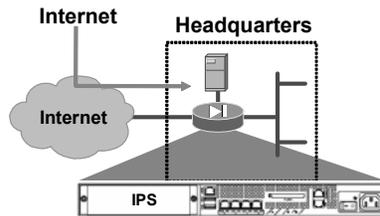
- IPS**: Keyword to set intrusion prevention services policy**
- **Define AIP-SSM operation**
  - **Inline mode—Directs packets to the ATIP-SSM**
  - **Promiscuous mode—duplicates packets and sends duplicates to the AIP-SSM**
- **Define action if AIP-SSM fails**
  - fail-close**—Blocks traffic if the AIP-SSM fails**
  - fail-open**—Permits traffic if the AIP-SSM fails**

SNPA v4.0—9-16

The Cisco ASA 5500 Series Adaptive Security Appliances support an optional Advanced Inspection and Prevention Security Services Module (AIP-SSM). IPS software can be loaded on the AIP-SSM card. The IPS software on the AIP-SSM card provides detailed deep packet stateful inspection on traffic flow designated by an intrusion prevention policy. The ASA Adaptive Security Appliance prefilters, then passes traffic to the IPS software on the AIP-SSM card for inspection and analysis. This level of interaction between the ASA Adaptive Security Appliance, the AIP-SSM, and IPS software allows the AIP-SSM to operate at greater efficiency because it only has to analyze a subset of the total bandwidth and because it reduces false-positive alarms by filtering out nonrelevant traffic.

The IPS software on the AIP-SSM card can operate in two modes:

- Promiscuous mode—In which the IPS software performs analysis on a copy of the filtered traffic instead of on the actual packet. A significant benefit of operating the IPS software in promiscuous mode is that the IPS software doesn't affect the flow of the actual packet. The drawback to operating in promiscuous mode is that the IPS software may not stop malicious traffic from reaching its intended target. The IPS software is analyzing a copy of the packet, so the response actions are sometimes post-event and often require assistance from other networking devices (for example, routers, security appliances) to respond to an attack.

- Inline mode—In which the IPS SOFTWARE performs analysis on the actual filtered traffic instead of a copy of the forwarded packet. An inline IPS SOFTWARE sits in the fast-path. allowing the sensor to stop attacks by dropping malicious traffic *before* it reaches the intended target. It is important to note that not only is the inline device processing information on the packet envelop (Layers 3 and 4), but it is also analyzing the contents and payload of the packets for more sophisticated embedded attacks (Layers 3 through 7). This deeper analysis allows the system to identify and stop or block attacks that might normally pass through a traditional firewall device. IPS software operating in inline mode is capable of stopping attacks instead of simply identifying them.

The other configurable parameters are **fail-open** and **fail-close**. These parameters determine what happens to the traffic flow if the IPS software or AIP-SSM fails for any reason (either hardware or software malfunction).

- **fail-open**: Traffic will continue to flow if the AIP-SSM fails; this is the default for AIP-SSMs operating in promiscuous mode.
- **fail-closed**: Traffic will cease flowing if the AIP-SSM fails for any reason.

Example: Intrusion Prevention Policy

Internet   **Headquarters**

Internet

IPS
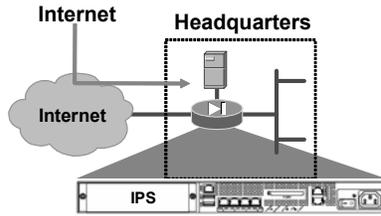
firewall(config)#

```
IPS {inline | promiscuous} {fail-close | fail-open}
```

- **Sends the Internet class of packets to the AIP-SSM**
- **If the AIP-SSM fails, permits traffic**

```
pix1(config)# policy-map outside_policy
pix1(config-pmap)# class internet
pix1(config-pmap-c)# IPS inline fail-open
```

SNPA v4.0—9-17

To configure the intrusion prevention action, you use the **IPS** command to configure two items, the AIP-SSM mode and the AIP-SSM failure action. In the example in the figure, the Internet class packets are forwarded to the AIP-SSM. The module is in inline mode so it performs analysis on the actual filtered traffic instead of on a copy of the forwarded packet. If the AIP-SSM fails, Internet traffic will continue to flow. This action, when enabled, is bidirectional.

The syntax of the **IPS** command is as follows:

```
IPS {inline | promiscuous} {fail-close | fail-open}
```

fail-close	Block traffic if the AIP-SSM module fails.
fail-open	Permit traffic if the AIP-SSM module fails.
inline	Direct packets to AIP-SSM module; the packet might be dropped as a result of IPS operation.
promiscuous	Duplicate packets for AIP-SSM module; the original packet cannot be dropped by AIP-SSM module.

Inspect Policy Overview

Internet   **Headquarters**

Inspect FTP

Internet
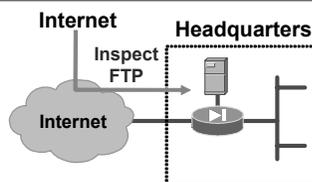
- inspect: **Keyword to set inspection policy**

```
pix1(config-pmap-c)# help inspect

USAGE:
        [no] inspect gtp <gtp_map>
        [no] inspect mgcp <mgcp_map>
        [no] inspect http <http_map>
        [no] inspect snmp <snmp_map>
        [no] inspect ftp [strict]
        [no] inspect icmp
        [no] inspect icmp error
        [no] inspect h323 ras|h225
        [no] inspect dns maximum-length <max_pkt_len>
        [no] inspect cuseeme|pptp|rpc|ctiqbe|ils|netbios|rsh|rtsp|sip|
                     skinny|esmtp|sqlnet|xdmcp|tftp
```

SNPA v4.0—9-18

Today, corporations that use the Internet for business transactions want to keep their internal networks secure from potential threats. These corporations usually implement security appliances as part of their network defense strategy. Security appliances can help protect their networks, but some security appliances may also cause problems. For example, applications such as File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), multimedia, and SQL*Net require their communications protocols to dynamically negotiate source or destination ports or IP addresses. Some security appliances cannot participate in these dynamic protocol negotiations, resulting in either the complete blockage of these corporate services or the need to preconfigure static "holes" in the security appliance to allow these services.

A good security appliance has to inspect packets above the network layer and do the following as required by the protocol or application:

- Securely open and close negotiated ports or IP addresses for legitimate client-server connections through the security appliance

- Use Network Address Translation (NAT)-relevant instances of IP addresses inside a packet

- Use port address translation (PAT)-relevant instances of ports inside a packet

- Inspect packets for signs of malicious application misuse

You can configure your security appliance to inspect the required protocols, or applications, and permit them to traverse the security appliance. This enables the corporation's networks to remain secure while conducting day-to-day business.

Priority Policy Overview

Headquarters

Internet

Site to Site

Site to Site

Site C

Site B
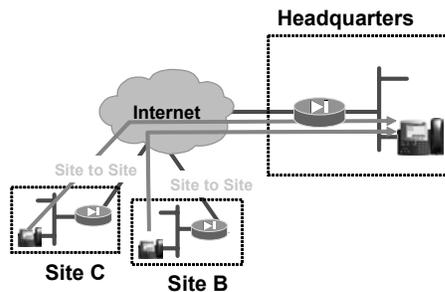
priority**: Keyword to set LLQ policy**

- **Identifies delay-sensitive, high-priority traffic flows**
- **Uses the** priority **command to enable LLQ queuing for the delay-sensitive traffic**

SNPA v4.0—9-19

As has video, Voice over IP (VoIP) has become one of the critical pieces emerging in the field of communications today. VoIP is relied upon more and more as a means of interoffice communication between geographically dispersed sites. To secure those communication channels, VPNs, which take advantage of the higher speed capabilities of cable and DSL, are replacing the common WAN infrastructure for speed, security, and cost-effectiveness . Quality of service (QoS) is the focal point to ensure that latency and jitter in VoIP traffic, which can adversely affect transmission quality, are minimized or eliminated to provide clear, uninterrupted voice and video communications while still providing a basic level of service for all other traffic passing through the device.

LLQ is implemented to prioritize packet transmission. There are two transmission queues in a security appliance: LLQ to handle priority traffic (voice and video) and a default queue to handle all other traffic. Use the **class-map** command to identify delay-sensitive traffic flows and priority traffic. Use the **priority** command to enable LLQ for the specific traffic transmit flows. This action, when enabled, is unidirectional.

Example: Priority Policy

Cisco.com

Headquarters

Internet

Site to Site

Site to Site

Site C

Site B
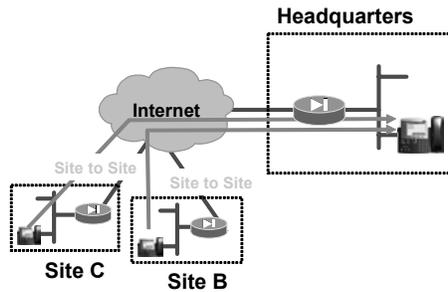
- **Sets LLQ policy for site-to-site voice traffic**

```
pix1(config)# policy-map outside_policy
pix1(config-pmap)# class s2s_voice
pix1(config-pmap-c)# priority
```

SNPA v4.0—9-20

In the example in the figure, there are two site-to-site VPN tunnels. The customer has both VoIP and data transmitting over the VPN tunnels. To ensure consistent good-quality voice transmission, the administrator has decided to route the voice traffic over the LLQ. To accomplish this policy, the priority LLQ is associated with the class s2s_voice traffic flow.

The syntax of the **priority** commands is as follows:

```
Priority
```

Priority	To apply strict scheduling priority for this class of traffic.

Set Policy Overview

Cisco.com

System Engineers   Internet   Headquarters

SE
exec

Executives   Internet

Site to Site   Site to Site

Site C   Site B
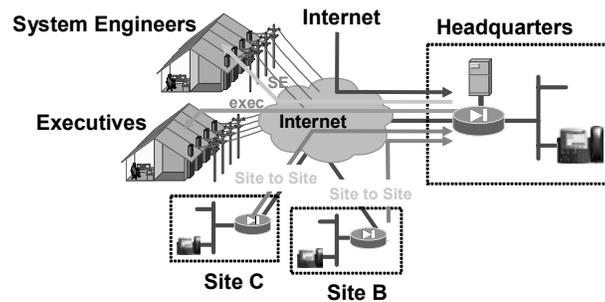
set connection**: Keyword to set connection policy**

• conn-max**—Maximum number of simultaneous connections that are allowed**
• embryonic-conn-max**—Maximum number of embryonic connections that are allowed**
• random-sequence**—Enables or disables TCP sequence number randomization**
• timeout**—Configures connection timeout parameters**

SNPA v4.0—9-21

Use the **set connection** command to configure general connection policies. When a connection matches the associated match criteria of this action, the security appliance sets the specified connection policy. This action, when enabled, is bidirectional.

The syntax for the **set connection** command is as follows:

```
set connection {conn-max | embryonic-conn-max } n timeout
random-seq# {enable | disable}
```

conn-max	The maximum number of simultaneous TCP and UDP connections that are allowed.
embryonic-conn-max	The maximum number of simultaneous embryonic connections that are allowed.
random-seq#	Enables or disables TCP sequence number randomization.
timeout	Configures connection timeout parameters.

Example: Set Policy

Internet   **Headquarters**

Internet
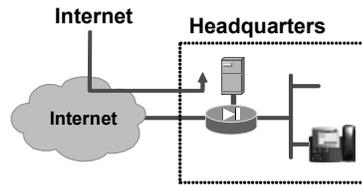
firewall(config)#

```
set connection {conn-max | embryonic-conn-max } n
  timeout random-seq# {enable | disable}
```

• **Sets the connection and embryonic-connection maximums for dmz server traffic**

```
pix1(config)# policy-map outside_policy
pix1(config-pmap)# class dmz_servers
pix1(config-pmap-c)# set connection conn-max 200
pix1(config-pmap-c)# set connection embryonic-conn-max 25
```

SNPA v4.0—9-22

The administrator wants to limit the number of connections and embryonic connections for the dmz_server class of traffic. In the example in the figure, the administrator has set the maximum connection number for the dmz_server class of traffic to 200 and the embryonic connection maximum to 25.

show run policy-map Command

Cisco.com

System Engineers — **Internet** — **Headquarters**

Executives

Site C   **Site B**
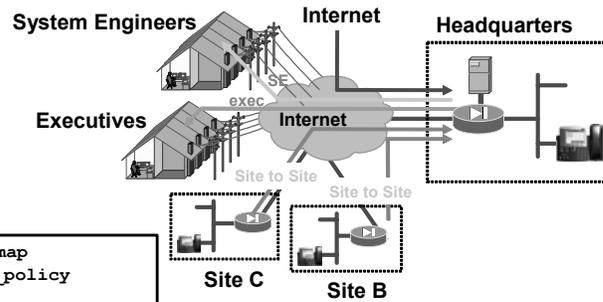
```
pix1# show run policy-map
   policy-map outside_policy
    class se
        police 56000 1000
    class exec
        police 56000 1000
    class s2s_voice
        priority
    class internet
        IPS inline fail-open
    class dmz_servers
        set connection conn-max 200
        embryonic-conn-max 25
```

SNPA v4.0—9-23

To display all the policy map configurations or the default policy map configuration, use the
show running-config policy-map command.

Configuring a Service Policy

This topic explains how to configure a service policy.

To activate a policy map globally on all interfaces or on a targeted interface, use the **service-policy** command in privileged EXEC mode. An interface can be a VLAN interface or a physical interface. In general, a **service-policy** command can be applied to any interface that can be defined by the **nameif** command. To disable, use the **no** form of this command. In the example in the figure, the administrator is activating the previously defined outside_policy policy map on the outside interface of the security appliance.

The syntax of the **service-policy** command is as follows:

service-policy *policymap_name* [global | interface *intf*]

policymap_name	A unique alphanumeric policy map identifier
global	Applies the policy map to all interfaces.
interface	Applies the policy map to a specific interface
intf	The interface name defined in the **nameif** command

show run service policy Command

Cisco.com

System Engineers

Executives

Internet

Headquarters

```
service-policy global_policy interface global
service-policy outside_policy interface outside
```
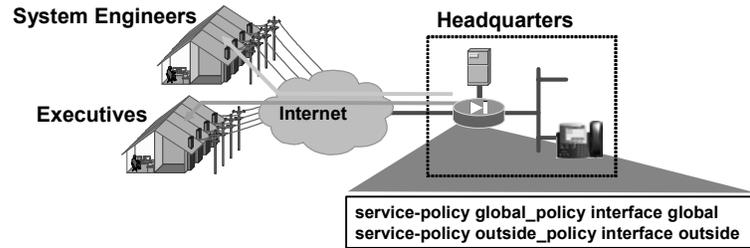
- **Shows the global policy security policy and the outside policy security policy**

```
pix1# Service-policy global_policy interface global
   service-policy global_policy global
   service-policy outside_policy interface outside
```

SNPA v4.0—9-26

To display all currently running service policy configurations, use the **show running-config service-policy** command in global configuration mode.

The syntax of the **show running-config service-policy** command is as follows:

```
show running-config [default] service-policy
```

| **default** | Displays the default service policy. |

Displaying Service Policies

```
pix1# show service-policy
Interface outside:
  Service-policy: outside_policy
    Class-map: se
      police:
          cir 56000 bps, bc 1000 bytes
        conformed 0 packets, 0 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        conformed 0 bps, exceed 0 bps
    Class-map: exec
      police:
          cir 56000 bps, bc 1000 bytes
        conformed 0 packets, 0 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        conformed 0 bps, exceed 0 bps
    Class-map: s2s
    Class-map: internet
      IPS: mode inline, packet 0
```

SNPA v4.0—9-27

To display the configured service policies with their corresponding classes and policies, use the **show service-policy** command in global configuration mode.

The syntax of the **show service-policy** commands is as follows:

```
show service-policy [global | interface intf ] [ action | flow
flow_description ]
```

global	When this keyword is specified, the policy map is referred to as a global policy map, that is, it applies to all interfaces. Only one global policy is allowed.
interface	When this keyword is specified, the policy map is referred to as an interface policy map, that is, it applies only to the interface specified.
intf	This specifies an interface name:
	If an interface name is specified, the policy map applies only to that interface. The interface name is defined in the **nameif** command.
	An interface policy map overrides a global policy map.
	Only one interface policy map is allowed per interface.
action	Specifies an action for which the statistics or operational data are to be shown.
flow	Show all the policies enabled on a flow.
inspect	Show status/statistics of 'inspect' policy
ips	Show status/statistics of 'ips' policy
police	Show status/statistics of 'police' policy
priority	Show status/statistics of 'priority' policy

Summary

This topic summarizes what you learned in this lesson.

Summary

Cisco.com

- **The Cisco Modular Policy Framework provides greater granularity and more flexibility for configuring network policies.**
- **Configure a class map by naming a class and specifying a matching class of traffic.**
- **Configure a policy map by identifying a class and associating a policy action to the class of traffic.**
- **Configure a service policy by identifying a policy name and applying the policy globally or to an interface.**

© 2005 Cisco Systems, Inc. All rights reserved.

SNPA v4.0—9-28

Lesson 10

Advanced Protocol Handling

Overview

This lesson introduces security appliance advanced protocol handling. The lesson explains how to configure an inspection modular policy, define an FTP map, and define an HTTP map and also describes a number of the inspection protocols supported by Cisco security appliances.

Objectives

Upon completing this lesson, you will be able to describe and configure security appliance advanced protocol handling. This ability includes being able to meet these objectives:

- Describe the need for advanced protocol handling
- Describe the **inspect** command
- Configure protocol inspection
- Describe how the security appliance implements FTP and HTTP protocol inspection
- Describe how the security appliance implements remote shell (rsh), SQL, SMTP, ICMP, SNMP protocol inspection.
- Describe the issues with multimedia applications
- Describe how the security appliance supports multimedia call control and audio sessions

Advanced Protocol Handling

This topic is an overview of advanced protocol handling.

Need for Advanced Protocol Handling

- **Some popular protocols or applications behave as follows:**
  - **They negotiate connections to dynamically assigned source and destination ports and IP addresses.**
  - **They embed source and destination port and IP address information above the network layer.**
- **A good security appliance has to inspect packets above the network layer and do the following as required by the protocol or application:**
  - **Securely open and close negotiated ports and IP addresses for legitimate client-server connections through the security appliance**
  - **Use NAT-relevant instances of IP addresses inside a packet**
  - **Use PAT-relevant instances of ports inside a packet**
  - **Inspect packets for signs of malicious application misuse**

SNPA v4.0—10-3

Today, corporations that use the Internet for business transactions want to keep their internal networks secure from potential threats. These corporations usually implement security appliances as part of their network defense strategy. Security appliances can help protect their networks; but some they may also cause problems. For example, applications such as File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), multimedia, and SQL*Net require their communications protocols to dynamically negotiate source or destination ports or IP addresses. Some security appliances cannot participate in these dynamic protocol negotiations, resulting in either the complete blockage of these corporate services or the need to preconfigure static "holes" in the security appliance to allow these services.

A good security appliance has to inspect packets above the network layer and do the following as required by the protocol or application:

- Securely open and close negotiated ports and IP addresses for legitimate client-server connections through the security appliance

- Use Network Address Translation (NAT)-relevant instances of IP addresses inside a packet

- Use port address translation (PAT)-relevant instances of ports inside a packet

- Inspect packets for signs of malicious application misuse

You can configure the Cisco PIX Security Appliances and Adaptive Security Appliances to inspect the required protocols or applications and permit them to traverse the security appliance. This enables the corporation's networks to remain secure while conducting day-to-day business.

inspect Command

Cisco.com

NO FTP Protocol Inspection

Server   Client

TCP S/21- C/2008
TCP S/20- ????

Data	Control		Control	Data
Port	Port		Port	Port
20	21		2008	2010

Port 2010

Port 2010 OK

Data X

No return port for data

FTP Protocol Inspection

Server   Client

TCP S/21- C/2008
TCP S/20- C/2010

Data	Control		Control	Data
Port	Port		Port	Port
20	21		2008	2010

Port 2010

Port 2010 OK

Data
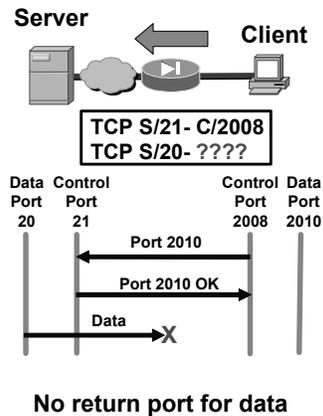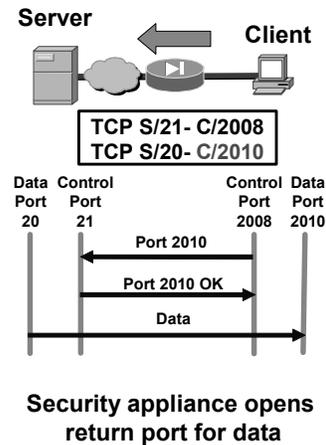
**Security appliance opens
return port for data**

SNPA v4.0—10-4

The advanced protocol inspection algorithm used by the security appliance for stateful application inspection ensures the secure use of applications and services. Some applications require special handling by the security appliance application inspection function. Applications that require special application inspection functions are those that embed IP addressing information in the user data packet or that open secondary channels on dynamically assigned ports. The application inspection function works with NAT to help identify the location of embedded addressing information. This allows NAT to translate these embedded addresses and to update any checksum or other fields that are affected by the translation.

The application inspection function also monitors sessions to determine the port numbers for secondary channels. Many protocols open secondary TCP or User Datagram Protocol (UDP) ports. The initial session on a well-known port is used to negotiate dynamically assigned port numbers. The application inspection function monitors these sessions, identifies the dynamic port assignments, and permits data exchange on these ports for the duration of the specific session. In the example in the figure, the FTP client is shown in active mode opening a control channel between its port 2008 and the FTP server port 21. When data is to be exchanged, the FTP client alerts the FTP server through the control channel that it expects the data to be delivered back from FTP server port 20 to its port 2010. If FTP inspection is not enabled, the return data from FTP server port 20 to FTP client port 2010 is blocked by the security appliance. With FTP inspection enabled, however, the security appliance inspects the FTP control channel to recognize that the data channel will be established to the new FTP client port 2010 and temporarily creates an opening for the data channel traffic for the life of the session.

Default Traffic Inspection and Port Numbers

```
fw1(config)# class-map inspection_default
fw1(config)# match ?
default-inspection-traffic  Match default inspection traffic:
                              ctiqbe----tcp--2748     dns-------udp--53
                              ftp-------tcp--21        gtp-------udp--2123,3386
                              h323-h225-tcp--1720      h323-ras--udp--1718-1719
                              http------tcp--80        icmp------icmp
                              ils-------tcp--389       mgcp------udp--2427,2727
                              netbios---udp--137-138   rpc-------udp--111
                              rsh-------tcp--514       rtsp------tcp--554
                              sip-------tcp--5060      sip-------udp--5060
                              skinny----tcp--2000      smtp------tcp--25
                              sqlnet----tcp--1521      tftp------udp--69
                              xdmcp-----udp--177
```

By default, protocol inspection is enabled. In the example in the figure, by default, the security appliance is configured to inspect the listed protocols on the specified TCP or UDP port numbers. For example, the security appliance inspects FTP traffic on TCP port 21.

Default Protocol Inspection Policy

Class Map

```
class-map inspection_default
 match default-inspection-traffic
!
policy-map global_policy
 class inspection_default
  inspect dns maximum length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect sunrpc
  inspect rsh
  inspect rtsp
  inspect sip
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect tftp
  inspect xdmcp
!
service-policy global_policy global
```

Policy Map

Service Policy

SNPA v4.0—10-6

By default, protocol inspection is enabled globally. The command **class-map inspection_default** identifies a class of traffic that matches the TCP and UDP port numbers delineated under the **default-inspection-traffic** parameter. The global_policy policy map associates protocol inspections to the inspection default class of traffic on which the inspections are to be performed. Lastly, the global_policy service policy is applied globally. No user intervention is required by the administrator to enable default inspections on a security appliance. The administrator can choose to modify the default class map, policy map, or service policy.

Delete Inspection for a Protocol

Client   **Server**
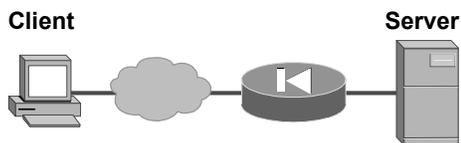
- **Disables ctiqbe protocol inspection**

```
fw1(config)# policy-map global_policy
fw1(config-pmap)# class inspection_default
fw1(config-pmap-c)# no inspect ctiqbe
fw1(config-pmap-c)# exit
fw1(config-pmap)# exit
```

SNPA v4.0—10-7

In the global_policy policy map, there is a default list of protocols that are inspected by the security appliance. You may choose to disable inspection of specific protocols by issuing the **no** form of the **protocol inspection** command. In the example in the figure, ctiqbe protocol inspection is disabled.

Add a Protocol Inspection Port Number

Server

Client

Inspect HTTP
Add TCP Port 8080
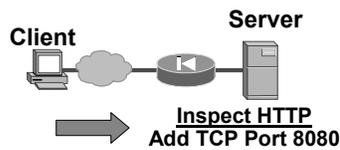
Adds port 8080 HTTP protocol inspection to a default policy map

- **Defines a class map to match the traffic flow identified by a port number, for example 8080**

- **Uses the policy map to associate the traffic flow, 8080, with a protocol inspection, inspect HTTP**

```
fw1(config)# class-map 8080_inspect_traffic
fw1(config-ftp-map)# match port tcp eq 8080
fw1(config-ftp-map)# exit
fw1(config)# policy-map global_policy
fw1(config-pmap)# class 8080_inspect_traffic fw1(config-pmap-c)# inspect http
fw1(config-pmap-c)# exit
fw1(config-pmap)# exit
```

SNPA v4.0—10-8

You may also choose to enable protocol inspection on an additional destination port number, for example, HTTP inspection on TCP port 8080. Adding protocol inspection to an additional port number is a two-step process. The first step is to identify traffic using a specific TCP and UDP destination port number in the **class-map** command, for example, TCP port 8080. Next, in a policy map, associate a policy with a class of traffic, for example, apply HTTP inspection to traffic that has TCP destination port 8080. These commands enable the security appliance to recognize that connections to port 8080 should be treated in the same manner as connections to HTTP port 80.

FTP Application Inspection

This topic discusses the configuration and handling of the FTP protocol inspection.

FTP Inspection

Cisco.com

- **FTP uses two channels:**
  - **Command connection (TCP)**
  - **Data connection (TCP)**
- **FTP inspection**
  - **Address translation in the message**
  - **Dynamic creation of openings for FTP data connections**
  - **Stateful tracking of request and response messages**
  - **(Optional) FTP strict, which prevents web browsers from sending embedded commands in FTP requests**
- **FTP deep packet inspection:**
  - **Is added to strict inspection functionality**
  - **Enables command filtering**

Server **Client**

Control Channel

Data

No Return Port for Data

SNPA v4.0—10-10

Cisco security appliances support application inspection for a large number of protocols, including FTP. FTP applications require special handling by the security appliance application inspection function. FTP applications embed data channel port information in the control channel traffic. The FTP inspection function monitors the control channel, identifies the data port assignment, and permits data exchange on the data port for the duration of the specific session. The example in the figure shows the FTP client opening a control channel between itself and the FTP server. When data is to be exchanged, the FTP client alerts the FTP server through the control channel that it expects the data to be delivered back from the FTP server port via a different port. If FTP inspection is not enabled, the security appliance blocks the return data from the FTP server port. With FTP inspection enabled, however, the security appliance inspects the FTP control channel, recognizes that the data channel will be established to the new FTP client port, and creates a temporary—for the life of the session—opening for the data channel traffic.

By default, the security appliance inspects port 21 connections for FTP traffic. The FTP application inspection involves inspecting the FTP sessions and performing four tasks:

■ Preparing dynamic secondary data connections

■ Tracking the **ftp** command-response sequence

■ Generating an audit trail

■ Preparing NAT-embedded IP addresses

If the **inspect ftp strict** option is enabled, each **ftp** command and response sequence is tracked for the following anomalous activity:

- Truncated command—Number of commas in the **port** and **pasv** reply commands is checked. If it is not five, then the **port** command is assumed to be truncated and the TCP connection is closed.

- Incorrect command—Checks the **ftp** command to see if it ends with **<CR><LF>** characters, as required by Request for Comments (RFC) standards. If it does not, the connection is closed.

- Size of **retr** and **stor** commands—These are checked against a fixed constant. If the size is greater, then an error message is logged and the connection is closed.

- Command spoofing—The **port** command should always be sent from the client. The TCP connection is denied if a **port** command is sent from the server.

- Reply spoofing—**pasv** reply command (227) should always be sent from the server. The TCP connection is denied if a **pasv** reply command is sent from the client. This prevents the security hole when the user executes "227 xxxxx a1, a2, a3, a4, p1, p2."

- Invalid port negotiation—The negotiated dynamic port value is checked to see if it is less than 1024. Port numbers in the range from 1 through 1023 are reserved for well-known connections, so if the negotiated port falls in this range, then the TCP connection is freed.

- Command pipelining—The number of characters present after the port numbers in the **port** and **pasv** reply commands is cross-checked with a constant value of 8. If it is more than 8, then the TCP connection is closed.

By filtering FTP request commands, administrators can further enhance inspection on FTP traffic to improve security and to control the service going through their security appliance. There is more on FTP command filtering later in this lesson.

Active Mode FTP Inspection

Cisco.com

- **Active mode FTP uses two channels:**
  - **Client-initiated command connection (TCP)**
  - **Server-initiated data connection (TCP)**
- **For outbound connections, the security appliance handles active mode FTP by opening a temporary inbound channel for the data.**
- **For inbound connections, if an FTP ACL exists, the security appliance handles active mode FTP as follows:**
  - **If outbound traffic is allowed, no special handling is required.**
  - **If outbound traffic is not allowed, it opens a temporary outbound connection for the data.**
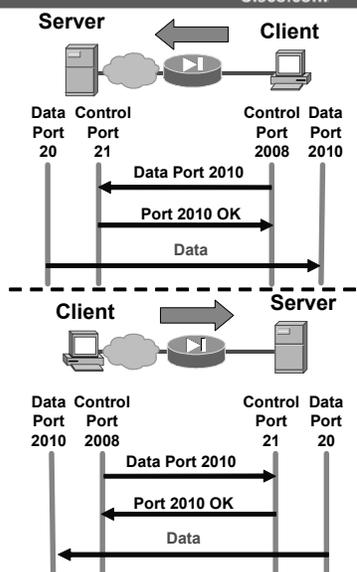
SNPA v4.0—10-11

Active mode FTP uses two channels for communications. When a client starts an FTP connection, it opens a TCP channel from one of its high-order ports to port 21 on the server. This is referred to as the control channel. When the client requests data from the server, it tells the server to send the data to a given high-order port. The server acknowledges the request and initiates a connection from its own port 20 to the high-order port that the client requested. This is referred to as the data channel.

Because the server initiates the connection to the requested port on the client, it has been difficult to have firewalls allow this data channel to the client without permanently opening port 20 connections from outside servers to inside clients for outbound FTP connections. This created a potential vulnerability by exposing clients inside the firewall. Protocol inspections have solved this problem.

For FTP traffic, the security appliance behaves in the following manner:

- Outbound connections: When the client requests data, the security appliance creates a temporary inbound opening for the data channel from the server. This opening is torn down after the data is sent.

- Inbound connections:

  — If an access control list (ACL) exists that allows inbound connections to an FTP server and if all outbound TCP traffic is implicitly allowed, no special handling is required because the server initiates the data channel from the inside.

  — If an ACL exists that allows inbound connections to an FTP server and if all outbound TCP traffic is *not* implicitly allowed, the security appliance creates a temporary opening for the data channel from the server. This opening is torn down after the data is sent.

Passive Mode FTP Inspection

- PFTP uses two channels:
  - Client-initiated command connection (TCP)
  - Client-initiated data connection (TCP)
- For outbound connections, the security appliance handles PFTP as follows:
  - If outbound traffic is allowed, no special handling is required.
  - If outbound traffic is not allowed, it opens an outbound port for the data channel.
- For inbound connections, if an FTP ACL exists, the security appliance opens an inbound port for the data channel.

SNPA v4.0—10-12
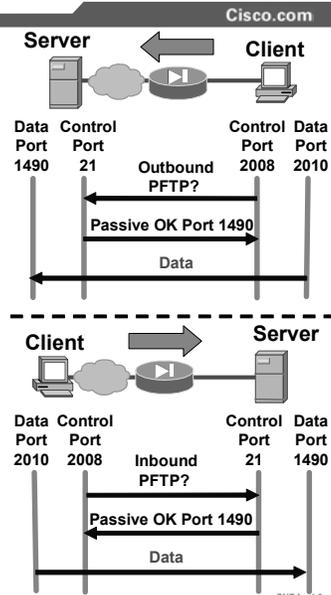
Passive mode FTP (PFTP) also uses two channels for communications. The command channel works the same as in an active mode FTP connection, but the data channel setup works differently. When the client requests data from the server, it asks the server if it accepts PFTP connections. If the server accepts PFTP connections, it sends the client a high-order port number to use for the data channel. The client then initiates the data connection from its own high-order port to the port that the server sent.

Because the client initiates the data connections and the command, early firewalls could easily support outbound connections without exposing inside clients to attack. Inbound connections, however, proved more of a challenge. The FTP inspection protocol resolved this issue.

For PFTP traffic, the security appliance behaves in the following manner:

- Outbound connections:

  — If all outbound TCP traffic is implicitly allowed, no special handling is required because the client initiates the data channels and the command from the inside.

  — If all outbound TCP traffic is not implicitly allowed, the security appliance creates a temporary opening for the data channel from the client. This opening is torn down after the data is sent.

- Inbound connections: If an ACL exists that allows inbound connections to a PFTP server, then when the client requests data, the security appliance creates a temporary inbound opening for the data channel that was initiated by the client. This opening is torn down after the data is sent.

Filtering Commands with FTP Deep Packet Inspection

Cisco.com

Client → **FTP Server**

FTP command filtering:
appe**: Append to a file**
cdup**: Change to parent of current directory**
⊘ dele**: Delete a file at the server site**
get**: Retrieve a file**
help**: Remote help information from server**
⊘ Mkd**: Create a directory**
⊘ put**: Store a file**
⊘ Rmd**: Remove a directory**
⊘ rnfr**: Rename from**
⊘ rnto**: Rename to**
site**: Specify server-specific command**
⊘ stou**: Store a file with a unique name**

- **Blocks specific commands within FTP requests**
- **Closes connection when an FTP command is filtered**
- **Is defined in the FTP-Map command**

SNPA v4.0—10-13

The existing FTP inspection allows FTP traffic by default and restricts only FTP traffic that fails security checks. FTP deep packet inspection enables you to block specific FTP request commands, such as renaming a file. When an FTP request command is filtered, the security appliance closes the connection. In the **ftp-map** command, you can define which FTP commands should be blocked. The FTP commands that you can block are:

- **appe**—Append to a file

- **cdup**—Change to parent of current directory

- **dele**—Delete a file

- **get**—Retrieve a file

- **help**—Remote help information from server

- **mkd**—Create a directory

- **put**—Store a file

- **rmd**—Remove a directory

- **rnfr**—Rename from

- **rnto**—Rename to

- **site**—Specify server-specific command

- **stou**—Store a file with a unique name

Configuring FTP Deep Packet Inspection

Client   FTP
                                            Server

Four-step process:

- ftp-map**: Defines which FTP request commands to filter**
- class-map**: Identifies a traffic flow**
- policy-map**: Associates FTP command filtering (**ftp-map**) with a traffic flow (**class-map**)**
- service-policy**: Applies policy to an interface, or globally.**

SNPA v4.0—10-14

To filter FTP commands, you must follow four steps. First, define in the **ftp-map** command which FTP commands you want to filter. Second, identify a traffic flow in the **class-map** command. Third, configure a policy that associates the FTP commands that are to be filtered (the **ftp-map** command) with the traffic flow that is identified in the class- map. And finally, use a service policy to enable the policy on an interface or on a global basis.

request-command deny Command

Client

FTP Server

fw1 (config-ftp-map)#

```
request-command deny { appe | cdup | dele | get |
  help | mkd | put | rmd | rnfr | rnto | site | stou }
```

- **Defines an FTP map name**
- **Identifies denied FTP request commands**

```
fw1(config)# ftp-map inbound_ftp
fw1(config-ftp-map)# request-cmd deny dele rnfr rnto appe put rmd
```

SNPA v4.0—10-15

To use the **ftp-map** command to define which FTP commands are to be blocked, follow these steps. Enter the **ftp-map** command and a map name; the system enters FTP map configuration mode. Use the **request-cmd deny** command to list which FTP request commands should be blocked. In the example in the figure, the inbound_ftp FTP map was defined. The inbound_ftp FTP map identifies six commands to be filtered: **dele**, **rnfr**, **rnto**, **appe**, **put**, and **rmd**. After an FTP map is configured, define a class map and a policy map, then apply the policy with a service policy.

The syntax for the **ftp-map** command is as follows:

```
ftp-map [map_name]
```

map_name	The name of the FTP map.

Example: FTP Inspection

Client

FTP Server

FTP Traffic

- **Define which FTP request commands to deny**
- **Identify traffic flow**
- **Define policy map**
  - **Class map: Identify a traffic flow**
  - **Associate FTP command filtering (FTP map) with traffic flow (class map)**
- **Apply policy to an interface**

```
fw1(config)# ftp-map inbound_ftp
fw1(config-ftp-map)# request-cmd deny dele rnfr rnto appe put rmd
fw1(config)# access-list 101 permit TCP any host 192.168.1.11 eq ftp
fw1(config)# class-map inbound_ftp_traffic
fw1(config-ftp-map)# match access-list 101
fw1(config-ftp-map)# exit
fw1(config)# policy-map inbound
fw1(config-pmap)# class inbound_ftp_traffic
fw1(config-pmap-c)# inspect ftp strict inbound_ftp
fw1(config-pmap-c)# exit
fw1(config-pmap)# exit
fw1(config)# service-policy inbound outside
```

SNPA v4.0—10-16

To deny FTP request commands, you must configure an FTP map, define a class map and a policy map, and apply the policy to an interface. The FTP map defines which FTP request commands should be blocked. The class map identifies a flow of traffic. The policy map associates the FTP map with a defined flow of traffic. The service policy enables the policy globally or on a specific interface. In the example in the figure, the inbound_ftp FTP map identifies six FTP request commands to filter. The inbound_ftp class of traffic matches traffic defined by ACL 101 (FTP traffic between any host and host 192.168.1.11, the FTP server). In the inbound policy map, the FTP command request restrictions defined in the inbound_ftp FTP map are associated with the inbound_ftp_traffic class of traffic. And finally, the inbound policy is enabled on the outside interface.

HTTP Application Inspection

This topic discusses the configuration and handling of the HTTP protocol inspection.

The **inspect http** command protects against specific attacks and other threats that may be associated with HTTP traffic. HTTP inspection performs several functions, as follows:

■ Checks whether an HTTP message is compliant to RFC standards. This includes checking the request message to ensure that it is one of the predefined methods: options, get, head, post, put, delete, trace, and connect. If the request messages does not contain one of these request methods, a check is made to verify that it is an extension method. If both the checks fail, then the user will be alerted. The default action is to generate a syslog message and reset the TCP connection.

■ Performs URL screening through N2H2 or Websense

■ Performs Java and ActiveX filtering

Note   The last two bulleted feature sets are configured in conjunction with the **filter** command. The **no inspect http** command statement also disables the **filter url** command.

■ Has enhanced HTTP inspection, which verifies that HTTP messages conform to RFC 2616, use RFC-defined methods or supported extension methods, and comply with various other configurable message criteria. In many cases, the administrator can configure these criteria and the system response when the criteria are not met.

By default, HTTP inspection is enabled globally. Inspection of HTTP port 80 traffic is defined in the inspection_default class map. In the global_policy policy map, HTTP inspection is associated with the inspection_default class of traffic, http port 80. HTTP inspection is enabled globally in the global_policy service policy. To remove HTTP inspection, use the **no** form of this command in the policy map.

The syntax for the **http-map** command is as follows:

```
inspect http [map_name]
```

map_name	The name of the HTTP map.

Enhanced HTTP Inspection

Client — HTTP Traffic → Web Server

- **Has the ability to control and filter HTTP traffic flowing through the security appliance**
  - **Checks whether HTTP message is RFC compliant**
  - **Specifies which RFC HTTP request methods are permitted**
  - **Specifies which extension methods are permitted**
  - **Specifies maximum header length for HTTP request and response messages**
  - **Specifies minimum and maximum content length**
  - **Confirms content-type in the message header is the same as the body of the HTTP message**
  - **Specifies maximum URI length in a request message**
  - **Specifies supported HTTP transfer-encoding type**
  - **Specifies supported MIME types**

SNPA v4.0—10-20

Enhanced HTTP inspection verifies that HTTP messages conform to RFC 2616, use RFC-defined methods or supported extension methods, and comply with various other criteria. In many cases, you can configure these criteria and the system response when the criteria are not met. The criteria that you can apply to HTTP messages include the following:

- Does not include any RFC or extension method on a configurable list

- Message body size is within configurable limits

- Request and response message header size is within a configurable limit

- Uniform resource identifier (URI) length is within a configurable limit

- The content type in the message body matches the header

- The content type in the response message matches the *accept-type* field in the request message

- The application type and transfer encoding are not restricted

To enable enhanced HTTP inspection, use the **inspect http** *http-map* command. The enhanced rules that apply to HTTP traffic are defined by the **http-map** command.

HTTP-Map: RFC and Extension Methods

Cisco.com

Client ——— **HTTP Traffic** ——→ **Web Server**

• **Define RFC and extension methods**

RFC Methods:	HTTP extention methods:	
connect	copy	revladd
delete	edit	revlabel
get	getattribute	revlog
head	getattributenames	revnum
options	getproperties	save
post	index	setattribute
put	lock	startrev
trace	Move	stoprev
	Mkdir	unedit
	default	unlock

• **Define an action upon receiving a restricted HTTP method**

fw1 (config-http-map)#

```
request-method { ext ext_methods | rfc rfc_methods }
  action | allow | drop | reset | [log]
```

SNPA v4.0—10-21

HTTP inspection verifies that HTTP messages conform to RFC 2616, use RFC-defined methods or supported extension methods. The RFC 2616 or supported extension methods must be one of the following:

■ RFC methods—connect | delete | get | head | options | post | put | trace | default

■ HTTP extension methods—index | move | mkdir | copy | default | edit | unedit | save | lock | unlock | index | move | revlabel | revlog | revadd | revnum | setattribute | getattribute | getproperties | startrev | stoprev |

You can define an **http-map** command to filter any of the above-mentioned methods. You can also define the actions of the security appliance upon receiving a restricted message: allow, send a TCP rest, close the connection, or send a syslog message.

The syntax for the **request-method** command is as follows:

```
request-method {{ext ext_methods | rfc rfc_methods} action | allow |
drop | reset | [log]
```

ext	Specifies extension methods
ext_method	Identifies one of the extended methods you want to allow to pass through the security appliance
rfc	Specifies RFC 2616-supported methods
rfc_method	Identifies one of the RFC methods you want to allow to pass through the security appliance
action	Identifies the action taken when a message fails this command inspection
allow	Allows the message
drop	Closes the connection
reset	Sends a TCP reset message to client and server
log	(Optional) Generates a syslog

HTTP Map Message Content Criteria

Client —— **HTTP Traffic** —→ **Web Server**

Define HTTP message content criteria:

- content-length**: Content length range inspection**
- content-type-verification**: Content type inspection**
- max-header-length**: Maximum header size inspection**
- max-uri-length**: Maximum URI size inspection**

fw1 (config-http-map)#

```
content-length { min bytes | max bytes] } action | allow | drop |
  reset | [log]
```

```
content-type-verification [match-req-rsp] action | allow | drop |
  reset | [log]
```

```
max-header-length {request bytes | response bytes} action | allow |
  drop | reset | [log]
```

```
max-uri-length bytes action | allow | drop | reset | [log]
```

SNPA v4.0—10-22

You can define message content criteria by placing bounds on the content length, header length, and URI length. You can also enable a check to verify that the content-type field in the HTTP response matches the accept field in the corresponding HTTP request message. In addition to defining the message criteria, you can define the actions to be performed when a message fails the defined message content criteria.

The message content criteria are as follows:

- **content-length**—To limit the HTTP traffic allowed through the security appliance based on the length of the entity body in the HTTP message. Messages within the configured range will be allowed; for all others, the configured action will be taken.

   — **min**—Minimum content length allowed; range is 0 to 65535 bytes

   — **max**—Maximum content length allowed; range is 0 to 50,000,000 bytes

The syntax for the **content-length** command is as follows:

```
content-length { min bytes | max bytes } action | allow | drop | reset
| [log]
```

min	Specifies the minimum content length allowed.
max	(Optional) Specifies the maximum content length allowed.
bytes	Number of bytes; range is 0 to 65535
action	The action taken when a message fails this command inspection
allow	Allows the message
drop	Closes the connection
reset	Sends a TCP reset message to client and server
log	(Optional) Generates a syslog

- **content-type-verification**—To enable a check that verifies that the content-type field in the HTTP response matches the accept field in the corresponding HTTP request message. If the message fails the checks, the configured action will be taken.

The syntax for the **content-type-verification** command is as follows:

```
content-type-verification [match-req-rsp] action {allow | reset |
drop}[log]
```

match-req-rsp	(Optional) Verifies that the content-type field in the HTTP response matches the accept field in the corresponding HTTP request message
action	The action taken when a message fails this command inspection
allow	Allows the message
drop	Closes the connection
reset	Sends a TCP reset message to client and server
log	(Optional) Generates a syslog

- **max-header-length**—To limit the HTTP traffic allowed through the security appliance by header length. Messages with header length less than or equal to the configured value will be allowed; for all others, the configured action will be taken.

    — bytes—Number of bytes; range is 0 to 65535

The syntax for the **max-header-length** command is as follows:

```
max-header-length {request bytes | response bytes} action | allow |
drop | reset | [log]
```

request	Request message
response	(Optional) Response message
bytes	Number of bytes; range is 0 to 65535
action	The action taken when a message fails this command inspection
allow	Allows the message
drop	Closes the connection
reset	Sends a TCP reset message to client and server
log	(Optional) Generates a syslog

- **max-uri-length**—To limit the HTTP traffic that is allowed through the security appliance by the length of the URI in a request message. URIs with length less than or equal to the configured value will be allowed; for all others, the configured action will be taken.

    — bytes—Number of bytes; range is 0 to 65535

The syntax for the **max-uri-length** command is as follows:

```
max-uri-length bytes action | allow | drop | reset | [log]
```

bytes	Number of bytes, range is 0 to 65535.
action	The action taken when a message fails this command inspection.
allow	Allow the message.
drop	Close the connection
reset	Send a TCP reset message to client and server.
log	(Optional) Generate a syslog.

- **action**—Action taken when a message fails inspection
  - allow—Allows the message
  - drop—Closes the connection
  - reset—Sends a TCP reset message to client, server, or both
  - log—Generates a syslog message

HTTP Map Application and Encoding Inspection

Client ——— HTTP Traffic ———▶ Web Server

Define HTTP application and encoding inspection:

- port-misuse**: Application inspection**
- transfer-encoding**: Transfer encoding inspection**
- action**: Defines actions when a violation occurs.**

fw1 (config-http-map)#

```
port-misuse {im | p2p | tunneling} action | allow |
  drop | reset | [log]
```

```
transfer-encoding {chunked | compress | deflate | gzip |
  identity} action | allow | drop | reset | [log]
```

SNPA v4.0—10-23

You can define application and encoding inspection, and you can limit the HTTP traffic that is allowed through the security appliance by specifying a restricted application such as Kazaa, Gnutella, and so on. You can also define the supported HTTP transfer-encoding types through the security appliance, for example, chunked, deflate, and gzip. And in addition to defining the application and encoding inspections, you can define the actions to be performed when an application or encoding type in the configured category is detected. The application and encoding inspection are as follows:

- **port-misuse**—To limit the HTTP traffic that is allowed through the security appliance by specifying a restricted application category. When an application in the configured category is detected, the configured action will be taken.

    — **im**—Instant messaging application category. The applications checked for are:

        ■ Yahoo Messenger

    — **p2p**—Peer to peer application category. The applications checked for are:

        ■ Kazaa

        ■ Gnutella

    — **tunneling**—Tunneling application category. The applications checked for are:

        ■ AIM

        ■ HTTPort/HTTHost

        ■ GNU Httptunnel

        ■ GotoMyPC

        ■ Firethru

        ■ Http-tunnel.com Client.

        ■ MSN

The syntax for the **port-misuse** command is as follows:

```
port-misuse {im | p2p | tunneling} action | allow | drop | reset |
[log]
```

im	Instant messaging application inspection
p2p	Peer-to peer-application inspection
tunneling	Tunneling application inspection
action	The action taken when a message fails this command inspection
allow	Allows the message
drop	Closes the connection
reset	Sends a TCP reset message to client and server
log	(Optional) Generates a syslog

- **transfer-encoding**—To configure specific action for each of the supported HTTP transfer-encoding types through the security appliance. With this command, if a request message contains a transfer-encoding type that is configured, the configured action will be taken.

  — **chunked**—Message body is transferred as a series of chunks

  — **compress**—Unix file compression

  — **deflate**—zlib format (RFC 1950) and deflate compression (RFC 1951)

  — **gzip**—GNU zip (RFC 1952)

  — **default**—Specifies the default action to be performed when an unconfigured parameter in the category is detected

The syntax for the **transfer-encoding** command is as follows:

```
transfer-encoding {chunked | compress | deflate | gzip | identity |
default} action | allow | drop | reset | [log]
```

chunked	Identifies the transfer encoding type in which the message body is transferred as a series of chunks
compress	Identifies the transfer encoding type in which the message body is transferred using UNIX file compression
deflate	Identifies the transfer encoding type in which the message body is transferred using zlib format (RFC 1950) and deflate compression (RFC 1951)
gzip	Identifies the transfer encoding type in which the message body is transferred using GNU zip (RFC 1952)
identity	Identifies connections in the message body where no transfer encoding is performed
action	The action taken when a message fails this command inspection
allow	Allows the message
drop	Closes the connection
reset	Sends a TCP reset message to client and server
log	(Optional) Generates a syslog

- **action**—Action taken when an application in the configured category is detected
    - **allow**—Allows the message
    - **reset**—Sends a TCP reset message to client and/or server
    - **drop**—Closes the connection
    - **log**—Generates a syslog message

Enhanced HTTP Inspection Configuration

Four-step process:

- **HTTP map: Define HTTP message criteria**
- **Class map: Identify a traffic flow**
- **Policy map: Associate HTTP controls and filters (HTTP map) with a traffic flow (class map)**
- **Service policy: Apply policy to an interface or globally**

SNPA v4.0—10-24

Configuring enhanced HTTP inspection is a four-step process. The four steps in the process are as follows:

- Configure the **http-map** command to define the enhanced HTTP inspection parameters and the action to be performed when a parameter in the configured category is detected.

- Identify the flow of traffic by using the **class-map** command. Use the default class map, inspection_default. Or define a new traffic flow, for example, any hosts that are trying to access the corporate web server from the Internet.

- Associate the HTTP map with a class of traffic by using the **policy-map** command. Use the default policy map, global_policy. Or define a new policy, for example, an inbound traffic policy for any hosts that are trying to access the corporate web server from the Internet.

- Apply the policy to an interface or globally by using the **service-policy** command. Use the default service policy, global_policy. Or define a new service policy, for example, a service policy for all inbound Internet-sourced traffic, and apply the service- policy to the outside interface.

Example: Appling HTTP Inspection

- **Configure an HTTP map**
- **Identify traffic flow**
- **Define a policy map**
  - **Associate HTTP command filtering (HTTP map) with traffic flow (class map)**
- **Apply policy to an interface**

```
fw1(config)# http-map inbound_http
fw1(config-http-map)# request-method rfc delete action reset log
fw1(config-http-map)# request-method rfc post action reset log
fw1(config-http-map)# request-method rfc put action reset log
fw1(config-http-map)# content-type-verification match-req-rsp action reset log
fw1(config-http-map)# exit
fw1(config)# access-list 102 permit TCP any host 192.168.1.11 eq www
fw1(config)# class-map inbound_http_traffic
fw1(config-ftp-map)# match access-list 102
fw1(config-ftp-map)# exit
fw1(config)# policy-map inbound
fw1(config-pmap)# class inbound_http_traffic
fw1(config-pmap-c)# inspect http inbound_http
fw1(config-pmap-c)# exit
fw1(config-pmap)# exit
fw1(config)# service-policy inbound outside
```

SNPA v4.0—10-25

In the example in the figure, the administrator created a new modular policy for HTTP traffic from the Internet to the corporate web server with an IP address of 192.168.1.11, rather than modify the existing default global modular policy. To accomplish this, the administrator configured a new HTTP map, class map, policy map, and service policy. The administrator created an HTTP map, inbound_http. In the HTTP map, RFC request methods are restricted and message criteria are defined. In the class map, traffic flow to a web server with a matching ACL, ACL 102 is identified. In a new policy map, the actions in the new HTTP map are associated to traffic identified in the ACL. And finally, the new service policy is enabled on the outside interface.

Protocol Application Inspection

This topic discusses the configuration and handling of the remote shell (rsh) protocol, Structured Query Language (SQL), Simple Mail Transfer Protocol (SMTP), ICMP, and Simple Network Management Protocol (SNMP).
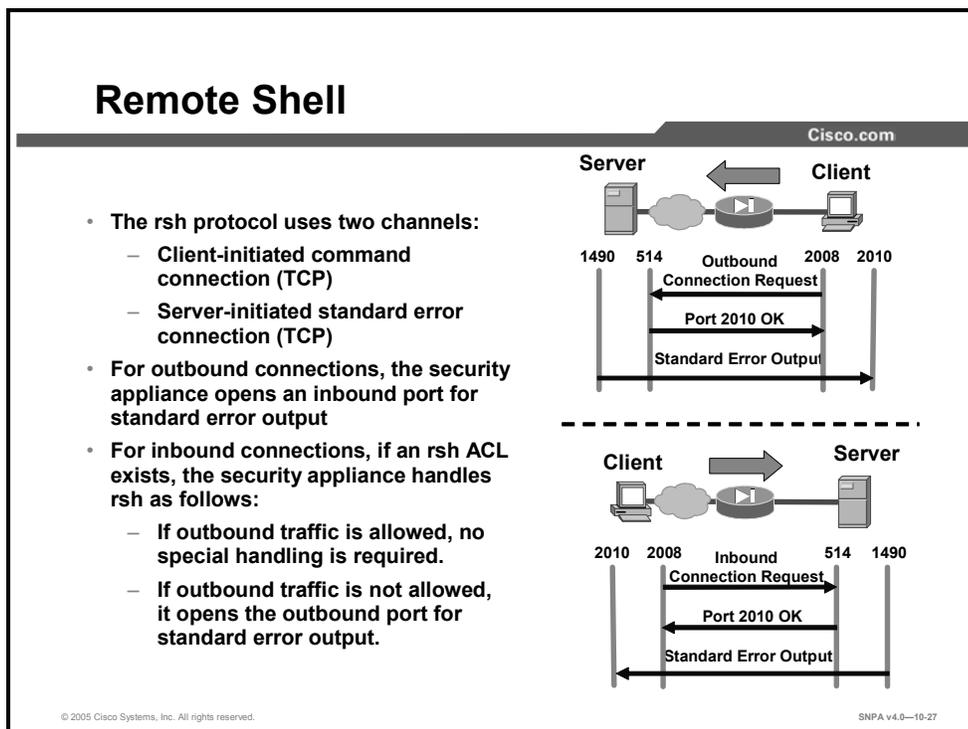
The rsh protocol uses two channels for communications. When a client first starts an rsh connection, it opens a TCP channel from one of its high-order ports to port 514 on the server. The server opens another channel for standard error output to the client.

For rsh traffic, the security appliance behaves in the following manner:

- Outbound connections: When standard error messages are sent from the server, the security appliance creates a temporary inbound opening for this channel. This opening is torn down when no longer needed.

- Inbound connections:

    — If an ACL exists that allows inbound connections to an rsh server and if all outbound TCP traffic is implicitly allowed, no special handling is required because the server initiates the standard error channel from the inside.

    — If an ACL exists that allows inbound connections to an rsh server and if all outbound TCP traffic is *not* implicitly allowed, the security appliance creates a temporary opening for the standard error channel from the server. This opening is torn down after the messages are sent.

By default, the security appliance inspects port 514 connections for rsh traffic. If you have rsh servers that are using ports other than port 514, you need to use the **class-map** command to identify these other traffic flows with their different rsh TCP port numbers. To enable rsh application inspection use the **inspect rsh** command in a policy map class configuration mode. To remove the rsh inspection, use the **no** form of this command.

The syntax for the **inspect rsh** command is as follows:

```
inspect rsh

no inspect rsh
```

SQL*Net

Server **Client**

- **Initially the client connects to a well-known port on the server.**
  - Oracle uses port 1521.
  - IANA-compliant applications use port 66.
- **The server may assign another port or another host to serve the client.**
- **For outbound connections, the security appliance handles SQL*Net connections as follows:**
  - **If outbound traffic is allowed, no special handling is required.**
  - **If outbound traffic is not allowed, it opens an outbound port for a redirected channel.**
- **For inbound connections, if an ACL exists, the security appliance opens an inbound port for a redirected channel.**
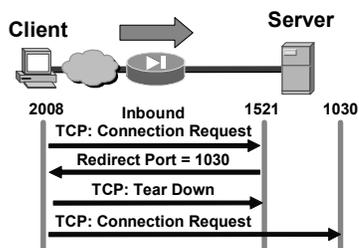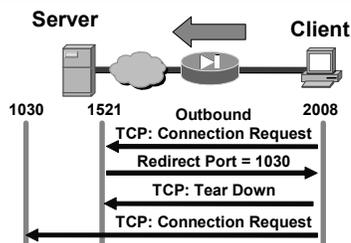
SNPA v4.0—10-28

SQL*Net only uses one channel for communications but it could be redirected to a different port, and even more commonly to a different secondary server altogether. When a client starts an SQL*Net connection, it opens a standard TCP channel from one of its high-order ports to port 1521 on the server. The server then proceeds to redirect the client to a different port or IP address. The client tears down the initial connection and establishes the second connection.

For SQL*Net traffic, the security appliance behaves in the following manner:

- Outbound connections:

  — If all outbound TCP traffic is implicitly allowed, no special handling is required because the client initiates all TCP connections from the inside.

  — If all outbound TCP traffic is *not* implicitly allowed, the security appliance opens an ACL for the redirected channel between the client and the server.

- Inbound connections: If an ACL exists that allows inbound connections to an SQL*Net server, the security appliance creates an inbound opening for the redirected channel.

By default, the security appliance inspects port 1521 connections for SQL*Net traffic. If you have SQL*Net servers using ports other than port 1521, you need to use the **class-map** command to identify these other traffic flows with their different SQL*Net port numbers. To enable SQL*Net application inspection, use the **inspect sqlnet** command in a policy map class configuration mode. To remove SQL*Net inspection, use the **no** form of this command. If the **inspect sqlnet** command is not enabled, then:

- Outbound SQL*Net will work properly on that port as long as outbound traffic is not explicitly disallowed.

- Inbound SQL*Net will *not* work properly on that port.

The syntax for the **inspect sqlnet** command is as follows:

```
inspect sqlnet
```

ESMTP Inspection

Mail Server

Client

Inbound SMTP Command
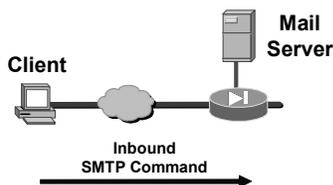
- **Allows only seven minimum SMTP commands:** helo, mail, rcpt, data, rset, noop, **and** quit **(RFC 821)**
- **Adds support for eight extended SMTP commands:** auth, data, ehlo, etrn, saml, send, soml, **and** vrfy
- **Defines ports on which to activate ESMTP inspection (default = 25)**
- **If disabled, all SMTP commands are allowed through the firewall; potential mail server vulnerabilities are exposed**

SNPA v4.0—10-29

Extended SMTP (ESMTP) is an enhancement to the SMTP protocol and is similar in most respects to SMTP. ESMTP application inspection provides improved protection against SMTP-based attacks by restricting the types of SMTP commands that can pass through the security appliance. ESMTP application inspection supports eight extended SMTP commands, including **auth**, **data**, **ehlo**, **etrn**, **saml**, **send**, **soml**, and **vrfy**, along with the support for seven RFC 821 commands, including **helo**, **help**, **mail**, **noop**, **quit**, **rcpt**, and **rset**. Cisco security appliances support a total of 15 SMTP commands.

The syntax for the **inspect esmtp** command is as follows:

```
inspect esmtp
```

DNS Inspection

DNS
Server   Client

UDP B/5 <- A/1050

53   1050
Request
Response
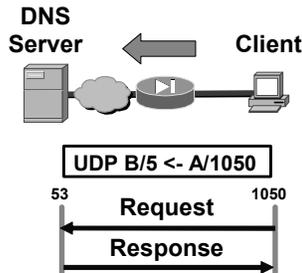
Monitors all UDP transactions on port 53:
• **Tracks DNS request ID and opens a connection slot**
• **Closes connection slot immediately after answer is received**
• **Translates the DNS A record**
  – **Before release 6.2:** alias **command**
  – **Release 6.2 and later: DNS record translation**
• **Reassembles the DNS packet to verify its length (default = 512 bytes)**

SNPA v4.0—10-30

The security appliance knows that Domain Name System (DNS) queries are a one-request, one-answer conversation, so the connection slot is released immediately after a DNS answer is received. When the DNS A record is returned, the security appliance applies address translation not only to the destination address, but also to the embedded IP address of the requested server address. This address is contained in the user data portion of the DNS reply packet. As a result, a web client on the inside network gets the address it needs to connect to the web server on the inside network. Prior to Cisco PIX Security Appliance Software v6.2, the PIX Security Appliance Software translated the embedded IP address with the help of the **alias** command. In PIX Security Appliance Software v6.2 and later, the security appliance has full support for NAT of embedded IP addresses within a DNS response packet.

Use the **inspect dns** command to specify the maximum DNS packet length.

The syntax for the **inspect dns** command is as follows:

```
inspect dns [maximum-length max_pkt_length]
```

This command is enabled by default. The default maximum length for the DNS packet size is 512.

DNS Record Translation
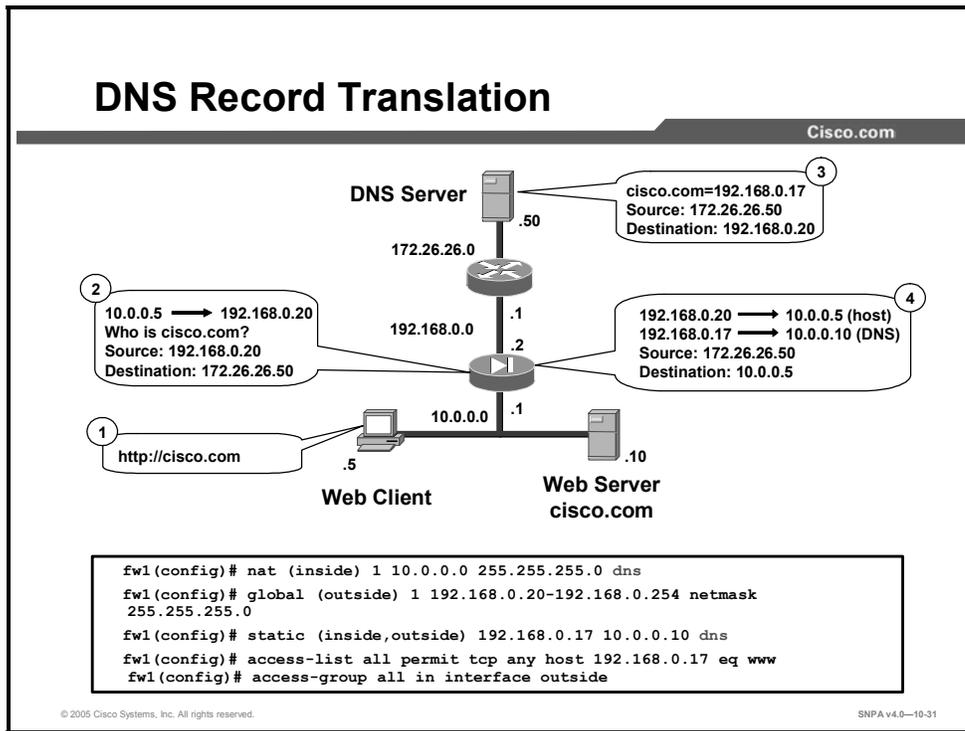
Cisco PIX Security Appliance Software v6.2 introduces full support for NAT of DNS messages originating from either inside (more secure) or outside (less secure) interfaces.

This means that if a client on an inside network requests DNS resolution of an inside address from a DNS server on an outside interface, the DNS A record is translated correctly. It is no longer necessary to use the **alias** command to perform DNS doctoring.

In the figure, the client on the inside network issues an HTTP request to server 10.0.0.10, using its hostname cisco.com. The security appliance translates the web client's nonroutable source address in the IP header and forwards the request to the DNS server on its outside interface. When the DNS A record is returned, the security appliance applies address translation not only to the destination address, but also to the embedded IP address of the web server. This address is contained in the user data portion of the DNS reply packet. As a result, the web client on the inside network gets the address it needs in order to connect to the web server on the inside network. NAT of DNS messages is implemented in both the **nat** and **static** commands. In the following **nat** and **static** command syntax, the location of the DNS keyword is highlighted:

```
nat [(interface)] nat_id address [netmask [outside] [dns]
[norandomseq] [timeout hh:mm:ss] [[tcp] [max_conns] [em_limit]]]

static [(prenat-interface, postnat-interface)] {mapped_address|
interface} real_address [dns] [netmask mask] [norandomseq] [[tcp]
[max_conns][em_limit]]
```

ICMP Inspection

172.26.26.50

Request

Reply → Insidehost

ICMP echo **request** (len 32 **id 512 seq 26624**) **Insidehost > 172.26.26.50**
ICMP echo **reply** (len 32 **id 512 seq 26624**) **172.26.26.50 > Insidehost**
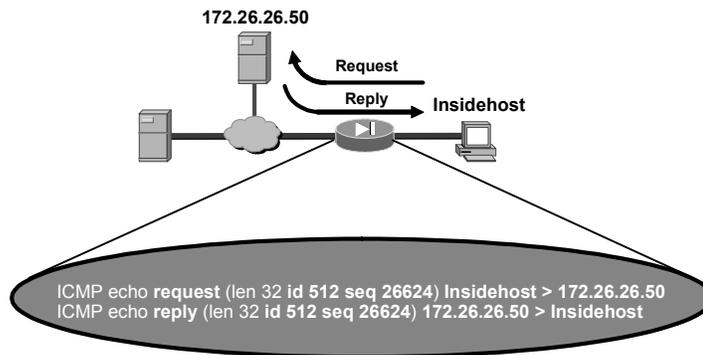
- **Purpose of ICMP inspection is to allow replies only when they match a request**
  - **Source, destination, ICMP type, identification number, sequence number**
  - **One request, one reply**

SNPA v4.0—10-32

Without ICMP stateful inspection, ICMP can be used to attack your network. ICMP inspection enables the security appliance to track ICMP traffic so it can be inspected like TCP and UDP traffic. For any single request, there will always be a single reply. When ICMP inspection is enabled, the ICMP payload is scanned to retrieve the pertinent information—source IP address, destination IP address, protocol, identification number, and sequence number—from the original packet. The idea is to match this session information in the security appliance for each ICMP request and response pair. ICMP inspection allows replies only when the ICMP reply session information matches a request. The ICMP inspection ensures that there is only one response for each request.

In the example in the figure, Insidehost is sending an ICMP request packet to the server at destination IP address 172.26.26.50. With ICMP inspection enabled, the security appliance tracks the information in the ICMP echo request, source, destination, protocol, identification number, and sequence number. ICMP inspection allows the ICMP reply from the server at 172.26.26.50 when it matches the original request.

To configure the ICMP inspection engine, use the **inspect icmp** command in policy map class configuration mode.

The syntax for the **inspect icmp** command is as follows:

```
inspect icmp [error]
```

SNMP Inspection

SNMP-Managed Device

.19 Traps

Internet

SNMP v1

10.0.0.11

SNMP manager 10.0.0.3
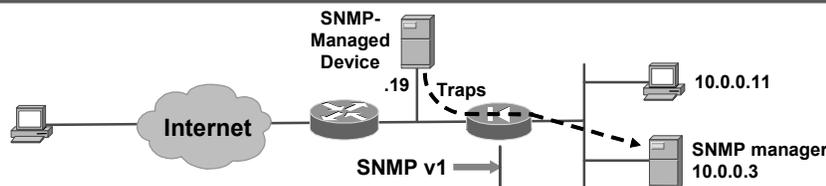
- snmp-map: **To deny a specific version of SNMP**
- inspect snmp: **To enable SNMP application inspection**

```
fw1(config)# snmp-map snmp_deny_v1
fw1(config-snmp-map)# deny version 1
fw1(config-snmp-map)# exit
fw1(config)# policy-map global_policy
fw1(config-pmap)# class snmp-port
fw1(config-pmap-c)# inspect snmp snmp_deny_v1
fw1(config-pmap-c)# exit
fw1(config-pmap)# exit
fw1(config)# service-policy global_policy global
```

SNPA v4.0—10-33

By default, the security appliance performs no inspection of SNMP traffic passing through the security appliance. The **SNMP-map** and **inspect snmp** commands can be used to filter out SNMP traffic based on the SNMP protocol version field in the packets, SNMP protocol versions 1, 2, 2c, or 3. Configuring SNMP version blocking is a two-step process, defining an SNMP map and applying the SNMP map to an SNMP inspection policy.

Use the **snmp-map** command to identify the SNMP protocol version(s) to deny. When you enter this command, the security appliance enters the snmp-map configuration mode. From the snmp-map configuration mode, you can define which SNMP protocol version to deny, version 1, 2, 2c, or 3. After defining the SNMP map, the administrator can apply the map parameters using the **inspect snmp** *map_name* command. The security appliance will inspect the SNMP traffic based on the contents of the snmp-map configuration.

To identify a specific map for defining the parameters for SNMP inspection, use the **snmp-map** *map_name* command. To remove the map, use the **no** form of this command. The syntax for the **snmp-map** *map_name* command is as follows:

snmp-map *map_name*

To enable SNMP inspection, use the **inspect snmp** *map_name* command in a policy map. To remove the configuration, use the **no** form of this command. The syntax for the **inspect snmp** *map_name* command is as follows:

```
inspect snmp map_name
```

Multimedia Support

This topic discusses multimedia: advantages and application supports, H.323 support, and important configurations.

Why Multimedia Is an Issue

Cisco.com

- **Multimedia applications behave in unique ways:**
  - **They use dynamic ports.**
  - **They transmit requests using TCP and get responses in UDP or TCP.**
  - **They use the same port for source and destination.**
- **The security appliance:**
  - **Dynamically opens and closes ports for secure multimedia connections**
  - **Supports multimedia with or without NAT**

TCP or UDP Request

Additional UDP or TCP high ports may be opened.

SNPA v4.0—10-35

Multimedia applications can transmit requests on TCP, get responses on UDP or TCP, use dynamic ports, use the same port for source and destination, and so on. Every application behaves in a different way. Implementing support for all multimedia applications using a single secure method is very difficult. Two examples of multimedia applications follow:

- RealAudio: Sends the originating request to TCP port 7070. The RealAudio server replies with multiple UDP streams anywhere from UDP port 6970 through 7170 on the client machine.

- Cisco IP Phone: Sends the Skinny Client Control Protocol (SCCP) messages to the call manager on TCP port 2000. SCCP uses Real-Time Transport Protocol (RTP) and Real-Time Control Protocol (RTCP) for media transmissions. The UDP media ports are randomly selected by the IP Phone.

The security appliance dynamically opens and closes UDP ports for secure multimedia connections. You do not need to open a large range of ports, which creates a security risk, nor do you have to reconfigure any application clients.

Also, the security appliance supports multimedia with or without NAT. Many security appliances that cannot support multimedia with NAT limit multimedia usage to only registered users or require exposure of inside IP addresses to the Internet. Lack of support for multimedia with NAT often forces multimedia vendors to join in proprietary alliances with security appliance vendors to accomplish compatibility for their applications.

- **RTSP uses one TCP and two UDP channels.**
- **Transport options:**
  - **RTP**
  - **RDP**
- **Sync or resend channel:**
  - **RTCP**
  - **UDP resend**

- **RTSP-TCP-only mode does not require special handling by the security appliance.**
- **Supported applications:**
  - **Cisco IP/TV**
  - **Apple QuickTime 4**
  - **RealNetworks:**
    - **RealAudio**
    - **RealPlayer**
    - **RealServer**

Real-Time Streaming Protocol (RTSP) is a real-time audio and video delivery control protocol used by many popular multimedia applications. It uses one TCP channel and multiple UDP channels. The TCP channel is the control channel and is used to negotiate the UDP delivery channels depending on the transport mode, RTP, or Session Description Protocol (SDP) that is configured on the client. RTSP applications use the well-known port 554, usually TCP, rarely UDP. Cisco security appliances support TCP only.

The first UDP channel is the data connection; it can use one of the following transport modes:

- RTP

- RealNetworks Real Data Transport Protocol (RDP)

The second UDP channel is a data connection feedback channel; it can use one of the following modes:

- RTCP

- UDP Resend

RTSP supports a TCP-only mode. This mode contains only one TCP connection, which is used as the control and data channels. Because this mode contains only one constant standard TCP connection, no special handling is required by the security appliance.

The following are RTSP applications that Cisco security appliances support:

- Cisco IP/TV
- Apple QuickTime 4
- RealNetworks
    — RealAudio
    — RealPlayer
    — RealServer

Note   RealNetworks RDP multicast is not supported.

Standard RTP Mode

Cisco.com

- **In standard RTP mode, RTP uses three channels:**
  - **Control connection (TCP)**
  - **RTP data (simplex UDP)**
  - **RTCP reports (duplex UDP)**
- **For outbound connections, the security appliance opens inbound ports for RTP data and RTCP reports.**
- **For inbound connections, if an ACL exists, the security appliance handles standard RTP mode as follows:**
  - **If outbound traffic is allowed, no special handling is required.**
  - **If outbound traffic is not allowed, it opens outbound ports for RTP and RTCP.**
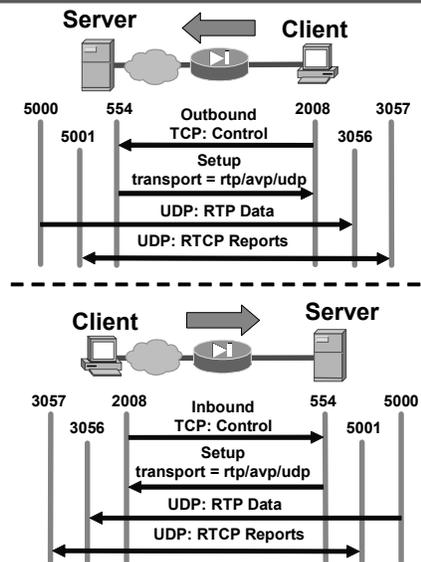
SNPA v4.0—10-37

In standard RTP mode, the following three channels are used by RTSP:

- TCP control channel: Standard TCP connection that is initiated from the client to the server.

- RTP data channel: Simplex (unidirectional) UDP session for media delivery that is using the RTP packet format from the server to the client. The client's port is always an even numbered port.

- RTCP reports: Duplex (bidirectional) UDP session that is used to provide synchronization information to the client and packet loss information to the server. The RTCP port is always the next consecutive port from the RTP data port.

For standard RTP mode RTSP traffic, the security appliance behaves in the following manner:

- Outbound connections: After the client and the server negotiate the transport mode and the ports to use for the sessions, the security appliance creates temporary inbound dynamic openings for the RTP data channel and RTCP report channel from the server.

- Inbound connections:

  — If an ACL exists that allows inbound connections to an RTSP server and if all outbound UDP traffic is implicitly allowed, no special handling is required because the server initiates the data and report channels from the inside.

  — If an ACL exists that allows inbound connections to an RTSP server and if all outbound TCP traffic is *not* implicitly allowed, the security appliance creates temporary dynamic openings for the data and report channels from the server.

RealNetworks RDP Mode

Cisco.com

Server **Client**

- In RealNetworks RDP mode, RTSP uses three channels:
  - Control connection (TCP)
  - UDP data (simplex UDP)
  - UDP resend (simplex UDP)

554 Outbound TCP: Control 2008

Setup
Transport = x-real-rdt/udp

UDP: Data

UDP: Resend

- For outbound connections, the security appliance handles RealNetworks RDP mode as follows:
  - If outbound traffic is allowed, it opens an inbound port for UDP data.
  - If outbound traffic is not allowed, it opens an inbound port for UDP data and an outbound port for UDP resend.

Client **Server**

- For inbound connections, if an ACL exists, the security appliance handles RealNetworks RDP mode as follows:
  - If outbound traffic is allowed, it opens an inbound port for UDP resend.
  - If outbound traffic is not allowed, it opens an outbound port for UDP data and an inbound port for UDP resend.

2008 Inbound TCP: Control 554

Setup
Transport = x-real-rdt/udp

UDP: Data

UDP: Resend

SNPA v4.0—10-38
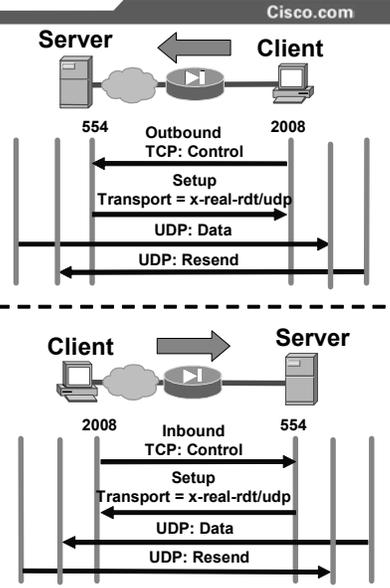
In RealNetworks RDP mode, the following three channels are used by RTSP:

- TCP control channel: Standard TCP connection that is initiated from the client to the server

- UDP data channel: Simplex (unidirectional) UDP session for media delivery that is using the standard UDP packet format from the server to the client

- UDP resend: Simplex (unidirectional) UDP session used for the client to request that the server resend lost data packets.

For RealNetworks RDP mode RTSP traffic, the security appliance behaves in the following manner:

- Outbound connections:

    — If outbound UDP traffic is implicitly allowed and after the client and the server negotiate the transport mode and the ports to use for the session, the security appliance creates temporary inbound openings for the UDP data channel from the server.

    — If outbound UDP traffic is *not* implicitly allowed and after the client and the server negotiate the transport mode and the ports to use for the session, the security appliance creates a temporary inbound opening for the UDP data channel from the server and a temporary outbound opening for the UDP resend channel from the client.

- Inbound connections:

    — If an ACL exists that allows inbound connections to an RTSP server and if all outbound UDP traffic is implicitly allowed, the security appliance creates a temporary inbound opening for the UDP resend from the client.

    — If an ACL exists that allows inbound connections to an RTSP server and if all outbound TCP traffic is *not* implicitly allowed, the security appliance creates temporary openings for the UDP data and UDP resend channels from the server and client, respectively.

RTSP Inspection

Client → **Server**   **Server** ← **Client**

2008   **Inbound**   554   554   **Outbound**   2008
TCP: Control   **TCP: Control**

Setup   **Setup**
Transport = x-real-rdt/udp   **Transport = x-real-rdt/udp**

UDP: Data   **UDP: Data**

UDP: Resend   **UDP: Resend**
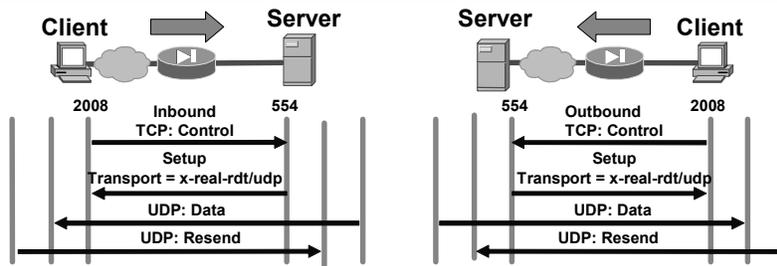
- **By default, the security appliance inspects RTSP connections.**
- **RTSP dynamically opens UDP connections as required.**
- **If disabled:**
  - **UDP transport modes are disallowed.**
  - **TCP transport modes are allowed (TCP connection rules apply).**

SNPA v4.0—10-39

By default, the security appliance inspects port 554 for RTSP connections. If you have devices in the network using ports other than port 554 for RTSP, you need to use the **class-map** command to identify these other traffic flows with their different RTSP port numbers. The **inspect rtsp** command causes the security appliance to create dynamic openings for UDP channels for RTSP traffic. Use the **no** form of the command to disable the inspection of traffic for RTSP connections. If the **inspect rtsp** command is not enabled, then neither outbound nor inbound RTSP will work properly on that port.

The syntax for the **inspect rtsp** command is as follows:

```
inspect rtsp

no inspect rtsp
```

H.323 Inspection

Gatekeeper   **Client**

1720   **H.225—Call signal**   2008
H.245—Capabilities
RTP Sessions
RTCP Session
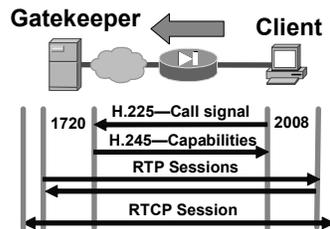
- **Defines ports for H.323 connections (default = 1720).**
- **H.323:**
  - **Uses signaling channel (H.225/Q.931)**
  - **Negotiates endpoint capabilities (H.245)**
  - **Opens dynamic media sessions (RTP/RTCP)**
- **If disabled, H.323 applications are disallowed.**

    SNPA v4.0—10-40

H.323 is more complicated than other traditional protocols because it uses two TCP connections and four to six UDP sessions for a single "call." (Only one of the TCP connections goes to a well-known port; all the other ports are negotiated and are temporary.) Furthermore, the content of the streams is far more difficult for security appliances to understand because H.323 encodes packets using Abstract Syntax Notation (ASN.1).

The call signaling function uses H.225 call signaling to establish a connection between two H.323 endpoints. In systems that do not have a gatekeeper, the call signaling channel is opened between the two endpoints that are involved in the call. In systems that contain a gatekeeper, the call signaling channel is opened between the endpoints and the gatekeeper or between the endpoints themselves as chosen by the gatekeeper. The security appliance dynamically allocates the H.245 connection based on the inspection of the H.225 messages.

The H.245 control function uses the H.245 control channel to carry end-to-end control messages governing operations of the H.323 entity, including capabilities exchange, opening and closing logical channels that carry the audiovisual and data information, mode preferences, and so on. The endpoint establishes one H.245 control channel for each call. The endpoints can establish multiple multimedia logical channels using RTP and RTCP. Within each H.245 message, the H.323 endpoints exchange port numbers that are used for subsequent UDP media streams. The H.323 inspection application inspects the H.245 messages to identify these ports and dynamically creates connections for the media exchange. RTP uses the negotiated port number, and RTCP uses the next-higher port number.

The H.323 control channel handles H.225, H.245, and H.323. H.323 inspection uses the following ports.

- 1718: Gatekeeper discovery UDP port

- 1719: Registration, admission, and status (RAS) UDP port

- 1720: TCP control port

The two major functions of H.323 inspection are as follows:

- Perform NAT on the necessary embedded IP v4 addresses in the H.225 and H.245 messages. Because H.323 messages are encoded in packed encoding rules (PER) format, the security appliance uses an ASN.1 decoder to decode the H.323 messages.

- Dynamically allocate the negotiated H.245, RTP, and RTCP connections.

The syntax for the **inspect h323** command is as follows:

```
inspect h323 [h225 | ras]

no inspect h323 [h225 | ras]
```

h225	Specifies the use of H.225, which is the ITU standard that governs H.225.0 session establishment and packetization, with H.323. H.225.0 actually describes several different protocols: RAS, use of Q.931, and use of RTP.
ras	Specifies the use of RAS with H.323 to enable dissimilar communication devices to communicate with each other. H.323 defines a common set of coder-decoders (codecs), call setup and negotiating procedures, and basic data transport methods.

By default, the security appliance inspects port 1720 connections for H.323 traffic. If there are network devices using ports other than the default ports, you need to use the **class-map** command to identify these other traffic flows with their different port numbers. Use **no inspect h323** command to disable the inspection of traffic for H.323 connections.

Cisco security appliances support H.323 v1 through v4 messages as well as the H.323 v3 feature Multiple Calls on One Call Signaling Channel.

SIP Inspection

IP Phone **IP Phone**

5060 Outbound SIP 2008

RTP
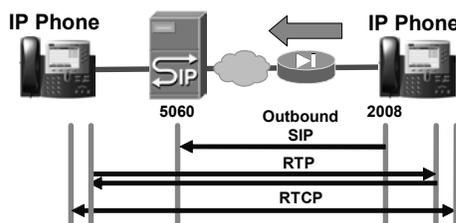
RTCP

- **Enables SIP**
- **Default port = 5060**
- **Enables security appliance to support any SIP VoIP gateways and VoIP proxies**
  - **Signaling mechanism (SIP)**
  - **Multimedia (RTP, RTCP)**

SNPA v4.0—10-41

Session Initiation Protocol (SIP) is an application-layer control protocol used to set up and tear down multimedia sessions. These multimedia sessions include Internet telephony and similar applications. SIP uses RTP for media transport and RTCP for providing a quality of service (QoS) feedback loop. Using SIP, your security appliance can support any SIP Voice over IP (VoIP) gateways and VoIP proxy servers.

To support SIP calls through the security appliance, signaling messages for the media connection addresses, media ports, and embryonic connections for the media must be inspected because although the signaling is sent over a well-known destination port (UDP/TCP 5060), the media streams are dynamically allocated. The **inspect sip** command can be used to enable or disable SIP support. SIP is a text-based protocol and contains IP addresses throughout the text. With the SIP inspection enabled, the security appliance inspects the packets, and both NAT and PAT are supported.

By default, the security appliance inspects port 5060 connections for SIP traffic. If there are network devices using ports other than the default ports, you need to use the **class-map** command to identify these other traffic flows with their different port numbers. Use **no inspect SIP** command to disable the inspection of traffic for SIP connections. The **show conn state sip** command can be used to display all active SIP connections.

The **timeout** command with the **sip media** option modifies the duration for the SIP media inactivity timer. When this time elapses, SIP connections with RTP and RTCP expire. The **timeout** command with the **sip** option modifies the duration for the SIP inactivity timer. When this time elapses, the port that is used by the SIP service closes.

Note   The security appliance also supports SIP proxies.

SCCP Inspection

SOHO
IP Phone   **PIX Firewall 501**

Cisco CallManager

	IP Phone to Cisco CallManager	
6058	Cisco CallManager to IP Phone	2000
	RTP	
	RTCP	
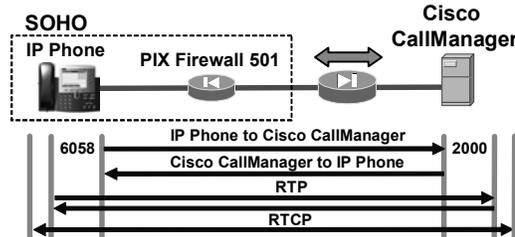
- **Supports SCCP used by Cisco IP Phones**
- **Enables SCCP signaling and media packets to traverse the security appliance (default port 2000)**
- **Dynamically opens negotiated ports for media sessions**
- **Can coexist in an H.323 environment**

SNPA v4.0—10-42

In Cisco PIX Security Appliance Software v6.0 and higher, the security appliance application handling supports SCCP, used by Cisco IP Phones for VoIP call signaling. SCCP defines the set of messages that is needed for a Cisco IP Phone to communicate with the Cisco CallManager for call setup. The IP Phone uses a randomly selected TCP port to send and receive SCCP messages. Cisco CallManager listens for SCCP messages at TCP port 2000. SCCP uses RTP and RTCP for media transmissions. The media ports are randomly selected by the IP Phones.

SCCP inspection enables the security appliance to dynamically open negotiated ports for media sessions. An application layer ensures that all SCCP signaling and media packets can traverse the security appliance and interoperate with H.323 terminals. SCCP support allows an IP Phone and Cisco CallManager to be placed on separate sides of the security appliance.

Skinny protocol inspection is enabled by default to listen for SCCP messages on port 2000. If there are network devices using ports other than the default ports, you need to use the **class-map** command to identify these other traffic flows with their different port numbers. Use the **no inspect skinny** command to disable SCCP traffic inspection.

The syntax for the **inspect skinny** command is as follows:

```
inspect skinny

no inspect skinny
```

CTIQBE Inspection

SOHO
SoftPhone   **PIX Firewall 501**

Cisco CallManager

6058	IP Phone to Cisco CallManager	2748
	Cisco CallManager to IP Phone	
	RTP	
	RTCP	
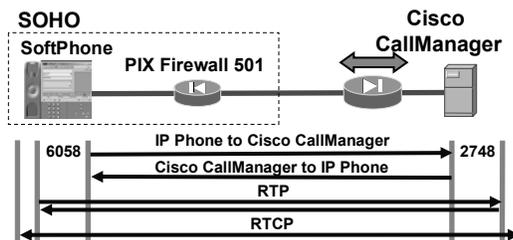
- **Supports CTIQBE protocol used by Cisco IP SoftPhones for desktop or laptop PC applications, such as collaboration**
- **Enables signaling and media packets to traverse the security appliance (default port 2748)**
- **Dynamically opens negotiated ports for media sessions**
- **Support disabled by default**

SNPA v4.0—10-43

The Telephony Application Programming Interface (TAPI) and Java TAPI (JTAPI) are used by many Cisco VoIP applications. Cisco PIX Security Appliance Software v6.3 introduces support for a specific protocol, Computer Telephony Interface Quick Buffer Encoding (CTIQBE), which is used by the Cisco TAPI service provider to communicate with Cisco CallManager. Support for this protocol is disabled by default.

By default, the security appliance inspects port 2748 connections for CTIQBE traffic. If there are network devices using ports other than the default ports, you need to use the **class-map** command to identify these other traffic flows with their different port numbers. Use the **no inspect ctiqbe** command to disable the inspection of traffic for CTIQBE connections.

The syntax for this command is as follows:

```
inspect ctiqbe
```

MGCP Inspection

Call Agent

Media Gateway

192.168.1.115

10.0.1.5

10.0.1.7

2427

Gateway to Call Agent

Call Agent to Gateway
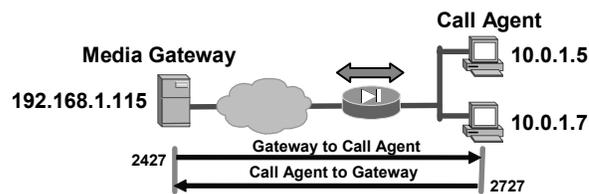
2727

- **Inspects messages passing between call agents and media gateways**
  - **Port 2427 on which gateway receives commands**
  - **Port 2727 on which call agent receives commands**
- **Dynamically opens negotiated ports for media sessions**
- **With multiple call agents configured, connections are opened for all the call agents configured for a particular MGCP gateway group**

SNPA v4.0—10-44

Cisco PIX Security Appliance Software v6.3 introduces support for application inspection of Media Gateway Control Protocol (MGCP). MGCP is used for controlling media gateways from external call control elements called media gateway controllers or call agents. A media gateway is typically a network element that provides conversion between the audio signals carried on telephone circuits and the data packets carried over the Internet or over other packet networks. Examples of media gateways are:

- Trunking gateway: Provides an interface between the telephone network and a VoIP network. Such gateways typically manage a large number of digital circuits.

- Residential gateway: Provides a traditional analog (RJ-11) interface to a VoIP network. Examples of residential gateways include cable modems and cable set-top boxes, DSL devices, and broadband wireless devices.

- Business gateway: Provides a traditional digital PBX interface or an integrated soft PBX interface to a VoIP network. MGCP messages are transmitted over UDP.

To use MGCP, you typically need to configure at least two ports, one on which the gateway receives commands and one for the port on which the call agent receives commands. Normally, a call agent will send commands to port 2427, and a gateway will send commands to port 2727. Audio packets are transmitted over an IP network using RTP. MGCP inspection enables the security appliance to securely open negotiated UDP ports for legitimate media connections through the security appliance.

Neither NAT nor PAT is supported by Cisco PIX Security Appliance Software v6.3 or lower.

MGCP Configuration

Call Agent

Media Gateway

10.0.1.5 Group 101

192.168.1.115
Group 101

10.0.1.7 Group 101

2427

Gateway to Call Agent

Call Agent to Gateway

2727

fw1 (config-mgcp-map)#

```
call-agent ip_address group_id
gateway ip_address group_id
```

```
fw1(config)# mgcp-map mgcp_policy
fw1(config-mgcp-map)# call-agent 10.0.1.5 101
fw1(config-mgcp-map)# call-agent 10.0.1.7 101
fw1(config-mgcp-map)# gateway 192.168.1.115 101
fw1(config-mgcp-map)# exit
fw1(config)# policy-map global_policy
fw1(config-pmap)# class inspection_default
fw1(config-pmap-c)# inspect mgcp mgcp_policy
fw1(config-pmap-c)# exit
```

SNPA v4.0—10-45

MGCP messages are transmitted over UDP. When an MGCP gateway sends a command to the call agent, it might not receive a response from the same call agent that the command was sent to. Multiple call agents can be configured. If multiple call agents are configured, connections are opened for all the call agents configured for a particular MGCP gateway (*group_id*). Use the **mgcp-map** command and subcommands to configure **call-agent**, **gateway**, and **command-queue**.

The syntax for the **mgcp-map** command is as follows:

mgcp-map [*map_name*]

map_name	The name of the FTP map.

The syntax for the **call-agent** command is as follows:

call-agent [*ip_address*] [*group_id*]

group_id	ID of the call agent group; range is 0 through 2147483647
ip_address	The IP address of the call agent

The syntax for the **gateway** command is as follows:

gateway [*ip_address*] [*group_id*]

group_id	ID of the call agent group; range is 0 through 2147483647
ip_address	The IP address of the call agent

The syntax for the **command-queue** command is as follows:

```
Command-queue [limit]
```

limit	Maximum number of commands to queue, range 1-2147483647.

In the example in the figure, there is a media gateway, 192.168.1.115, and two call agents, 10.0.1.5 and 10.0.1.7. Using the **mgcp-map** command, the administrator identifies the gateway, its IP address and group ID, the call agents, their IP address and group ID, and the maximum size of the command queue. The parameters configured in the **mgcp-map** command are applied to the **inspect mgcp** command in the security appliance default policy map. When the MGCP gateway sends a command to the call agents, it might not receive a response from the same call agent that the command was sent to. Multiple call agents are configured. With multiple call agents configured, connections are opened for all the call agents that are configured for a particular MGCP gateway, group 101 for example.

show run Command

```
class-map inspection_default
 match default-inspection-traffic
!
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp strict inbound_ftp
  inspect h323 h225
  inspect h323 ras
  inspect http inbound_http
  inspect mgcp mgcp_policy
  inspect netbios
  inspect sunrpc
  inspect rsh
  inspect rtsp
  inspect sip
  inspect skinny
  inspect esmtp
  inspect snmp inbound_snmp
  inspect sqlnet
  inspect tftp
  inspect xdmcp
!
service-policy global_policy global
```

SNPA v4.0—10-46

You can use the **show run** command to view the class map, policy map, and service policy configurations. In the example in the figure, the administrator has added inspection maps to the default configuration.

show service_policy Command

```
fw1# show service-policy

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: dns, packet 0, drop 0, reset-drop 0
      Inspect: ftp strict inbound_ftp, packet 0, drop 0, reset-drop 0
      Inspect: h323 ras, packet 0, drop 0, reset-drop 0
      Inspect: rsh, packet 0, drop 0, reset-drop 0
      Inspect: sip, packet 0, drop 0, reset-drop 0
      Inspect: skinny, packet 0, drop 0, reset-drop 0
      Inspect: sunrpc, packet 0, drop 0, reset-drop 0
      Inspect: xdmcp, packet 0, drop 0, reset-drop 0
      Inspect: netbios, packet 0, drop 0, reset-drop 0
      Inspect: mgcp mgcp_policy, packet 0, drop 0, reset-drop 0
      Inspect: tftp, packet 0, drop 0, reset-drop 0
      Inspect: snmp, packet 0, drop 0, reset-drop 0
      Inspect: http inbound_http, packet 0, drop 0, reset-drop 0
      Inspect: h323 h225, packet 0, drop 0, reset-drop 0
```

The **show service_policy** command displays statistics for enabled inspection policies and their respective actions, such as the number of packets allowed, the number of packets dropped, and the number of TCP resets.

Summary

This topic summarizes what you learned in this lesson.

Summary

- **With the** inspect **command, you can enable, disable, or enhance the use of a protocol inspection.**
- **The security appliance uses special handling for some advanced protocols: FTP, HTTP, SNMP, and MGCP.**
- **The security appliance handles such multimedia protocols as RTSP, RTP, SCCP, SIP, MGCP, and H.323.**
- **You can change the port value for protocol inspection.**

SNPA v4.0—10-49

Lesson 11

VPN Configuration

Overview

This lesson covers the basics of IPSec and security appliance virtual private networks (VPNs) with a focus on security appliance gateway to security appliance gateway communications. The basics of how VPNs function are detailed, then an overview and the tasks necessary to configure VPN connection parameters on the security appliance are presented. The lesson concludes with a brief explanation on how to scale security appliance VPNs using Certificate Authorities (CAs).

Objectives

Upon completing this lesson, you will be able to configure Cisco security appliances for VPN connectivity. This includes being able to meet these objectives:

- Describe how security appliances enable a secure VPN
- Perform the tasks necessary to configure security appliance IPSec support
- Identify the commands to configure security appliance IPSec support
- Configure a VPN between security appliances

Secure VPNs

A VPN is a service that offers secure, reliable connectivity over a shared, public network infrastructure such as the Internet. Because the infrastructure is shared, connectivity can be provided at lower cost than existing dedicated private networks.

The security appliance is a powerful enabler of VPN services. The security appliance's high performance, conformance to open standards, and ease of configuration make it a versatile VPN gateway.
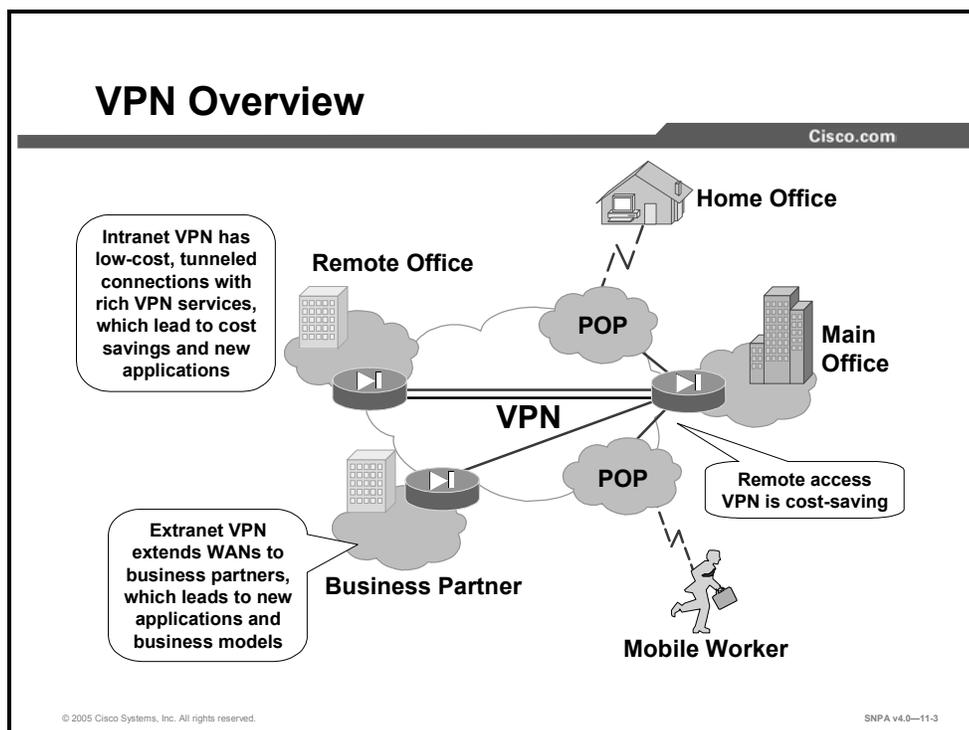
A VPN itself can be constructed in a number of scenarios. The most common are as follows:

- Internet VPN: A private communications channel over the public access Internet. This type of VPN can be divided into the following functions:

    — Connecting remote offices across the Internet

    — Connecting remote dial users to their home gateway via an ISP

- Intranet VPN: A private communication channel within an enterprise or organization that may or may not involve traffic traversing a WAN

- Extranet VPN: A private communication channel between two or more separate entities that may involve data traversing the Internet or some other WAN

In all cases, the VPN or tunnel consists of two endpoints that may be represented by security appliances, Cisco routers, individual client workstations running the Cisco VPN Client, or other vendors' VPN products that conform to open standards.

IPSec Enables Security Appliance VPN Features
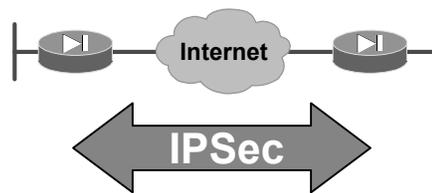
• **Data confidentiality**
• **Data integrity**
• **Data authentication**
• **Anti-replay**

SNPA v4.0—11-4

Cisco PIX Security Appliance Software v5.0 and higher use the industry-standard IPSec protocol suite to enable advanced VPN features.

IPSec provides a mechanism for secure data transmission over IP networks, ensuring confidentiality, integrity, and authenticity of data communications over unprotected networks such as the Internet.

IPSec enables the following security appliance VPN features:

■ Data confidentiality: The IPSec sender can encrypt packets before transmitting them across a network.

■ Data integrity: The IPSec receiver can authenticate IPSec peers and packets sent by the IPSec sender to ensure that the data has not been altered during transmission.

■ Data origin authentication: The IPSec receiver can authenticate the source of the IPSec packets that are sent. This service is dependent upon the data integrity service.

■ Anti-replay: The IPSec receiver can detect and reject replayed packets, helping to prevent spoofing and man-in-the-middle attacks.

What Is IPSec?
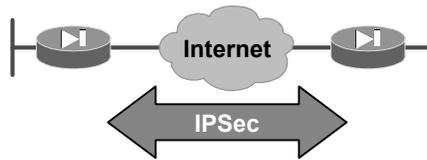
IETF standard that enables encrypted communication between peers

- **Consists of open standards for securing private communications**
- **Has network layer encryption that ensures data confidentiality, integrity, and authentication**
- **Scales from small to very large networks**
- **Is included in PIX Firewall v5.0 and later**

SNPA v4.0—11-5

Cisco security appliances use the open IPSec protocol to enable secure VPNs. IPSec is a set of security protocols and algorithms used to secure data at the network layer. IPSec and related security protocols conform to open standards promulgated by the Internet Engineering Task Force (IETF) and documented Request for Comments (RFCs) and IETF draft papers.

IPSec acts at the network layer, protecting and authenticating IP packets between a security appliance and other participating IPSec devices (peers), such as security appliances, Cisco routers, the Cisco VPN Client, and other IPSec-compliant products.

IPSec can be used to scale from small to very large networks. It is included in Cisco PIX Security Appliance Software v5.0 and later.

IPSec Standards Supported by the Security Appliance

- **IPSec**
  - **ESP**
- **IKE**
- **DES**
- **3DES**
- **AES**
- **DH**
- **MD5**
- **SHA**
- **RSA Signatures**
- **CAs**

Cisco security appliances support the following IPSec and related standards:

- IPSec

- Internet Key Exchange (IKE)

- Data Encryption Standard (DES)

- Triple Data Encryption Standard (3DES)

- Advanced Encryption Standard (AES)

- Diffie-Hellman (DH)

- Message Digest 5 (MD5)

- Secure Hash Algorithm-1 (SHA-1)

- Rivest, Shamir, and Adleman (RSA) Signature

- CA

IPSec

IPSec is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers at the IP layer. IPSec can be used to protect one or more data flows between IPSec peers. IPSec is documented in a series of Internet RFCs, all available at http://www.ietf.org/html.charters/ipsec-charter.html. The overall IPSec implementation is guided by RFC 2401, "Security Architecture for the Internet Protocol." IPSec consists of the following two main protocols:

- Authentication Header (AH): A security protocol that provides authentication and optional replay-detection services. AH acts as a "digital signature" to ensure that tampering has not occurred with the data in the IP packet. AH does not provide data encryption and decryption services. AH is not supported on your security appliance.

- **Encapsulating Security Payload (ESP):** A security protocol that provides data confidentiality and protection with optional authentication and replay-detection services. The security appliance uses ESP to encrypt the data payload of IP packets.

Internet Key Exchange

IKE is a hybrid protocol that provides utility services for IPSec: authentication of the IPSec peers, negotiation of IKE and IPSec security associations (SAs), and establishment of keys for encryption algorithms used by IPSec. IKE is synonymous with Internet Security Association and Key Management Protocol (ISAKMP) in security appliance configuration.

Data Encryption Standard

DES is used to encrypt and decrypt packet data. DES is used by both IPSec and IKE. DES uses a 56-bit key, ensuring high-performance encryption.

Triple Data Encryption Standard

3DES is a variant of DES that iterates three times with three separate keys, effectively doubling the strength of DES. 3DES is used by IPSec to encrypt and decrypt data traffic. 3DES uses a 168-bit key, ensuring strong encryption.

Advanced Encryption Standard

The National Institute of Standards and Technology (NIST) recently adopted the new AES to replace DES encryption in cryptographic devices. AES provides stronger security than DES and is computationally more efficient than 3DES. AES offers three different key strengths: 128-, 192-, and 256-bit keys.

Diffie-Hellman

DH is a public-key cryptography protocol. It enables two parties to establish a shared secret key over an insecure communications channel. DH is used within IKE to establish session keys.

Message Digest 5

MD5 is a hash algorithm used to authenticate packet data. The security appliance uses the MD5 Hash-based Message Authentication Code (HMAC) variant, which provides an additional level of hashing. A hash is a one-way encryption algorithm that takes an input message of arbitrary length and produces a fixed-length output message. IKE and ESP use MD5 for authentication.

Secure Hash Algorithm-1

SHA is a hash algorithm used to authenticate packet data. The security appliance uses the SHA-1 HMAC variant, which provides an additional level of hashing. IKE and ESP use SHA-1 for authentication.

RSA Signature

RSA is a public-key cryptographic system used for authentication. IKE on the security appliance uses a DH exchange to determine secret keys on each IPSec peer used by encryption algorithms. The DH exchange can be authenticated with RSA (or pre-shared keys).

Certificate Authority

The CA support of the security appliance enables the IPSec-protected network to scale by providing the equivalent of a digital identification card to each device. When two IPSec peers wish to communicate, they exchange digital certificates to prove their identities (thus removing the need to manually exchange public keys with each peer or to manually specify a shared key at each peer). The digital certificates are obtained from a CA. CA support on the security appliance uses Directory System Agent (DSA) Signature and RSA Signature to authenticate the CA exchange.

Security Association

The concept of an SA is fundamental to IPSec. An SA is a connection between IPSec peers that determines the IPSec services available between the peers, similar to a TCP or UDP port. Each IPSec peer maintains an SA database in memory containing SA parameters. SAs are uniquely identified by the IPSec peer address, security protocol, and security parameter index (SPI). You will need to configure SA parameters and monitor SAs on the security appliance.

How IPSec Works

This topic details the individual steps of IPSec.

Five Steps of IPSec

Host A   Security Appliance A   Security Appliance B   Host B

- **Interesting traffic: The VPN devices recognize the traffic to protect.**
- **IKE Phase 1: The VPN devices negotiate an IKE security policy and establish a secure channel.**
- **IKE Phase 2: The VPN devices negotiate an IPSec security policy to protect IPSec data.**
- **Data transfer: The VPN devices apply security services to traffic, then transmit the traffic.**
- **Tunnel terminated: The tunnel is torn down.**

SNPA v4.0—11-8

The goal of IPSec is to protect the desired data with the needed security services. IPSec operation can be broken down into five primary steps:

- Interesting traffic: Traffic is deemed interesting when the VPN device recognizes that the traffic you want to send needs to be protected.

- IKE Phase 1: A basic set of security services are negotiated and agreed upon between peers. These security services protect all subsequent communications between the peers. IKE Phase 1 sets up a secure communication channel between peers.

- IKE Phase 2: IKE negotiates IPSec SA parameters and sets up matching IPSec SAs in the peers. These security parameters are used to protect data and messages that are exchanged between endpoints.

- Data transfer: Data is transferred between IPSec peers based on the IPSec parameters and keys that are stored in the SA database.

- IPSec tunnel termination: IPSec SAs terminate through deletion or by timing out.

Step 1: Interesting Traffic

Host A   **Security Appliance A**   **Security Appliance B**   **Host B**

10.0.1.3   10.0.2.3

→ **Apply IPSec**

Send in Clear Text
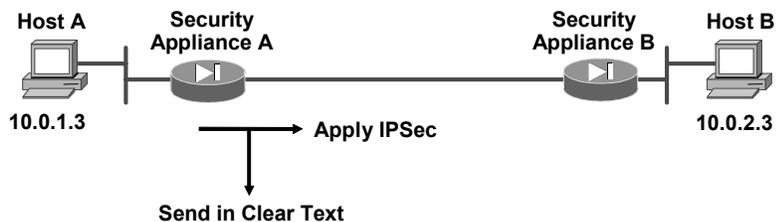
SNPA v4.0—11-9

Determining which traffic needs to be protected is done as part of formulating a security policy for use of a VPN. The policy is used to determine which traffic needs to be protected and which traffic can be sent in the clear. For every inbound and outbound datagram, there are two choices: apply IPSec or bypass IPSec and send the datagram in clear text. For every datagram protected by IPSec, the system administrator must specify the security services applied to the datagram. The security policy database specifies the IPSec protocols, modes, and algorithms that are applied to the traffic. The services are then applied to traffic destined to each particular IPSec peer.

Step 2: IKE Phase 1
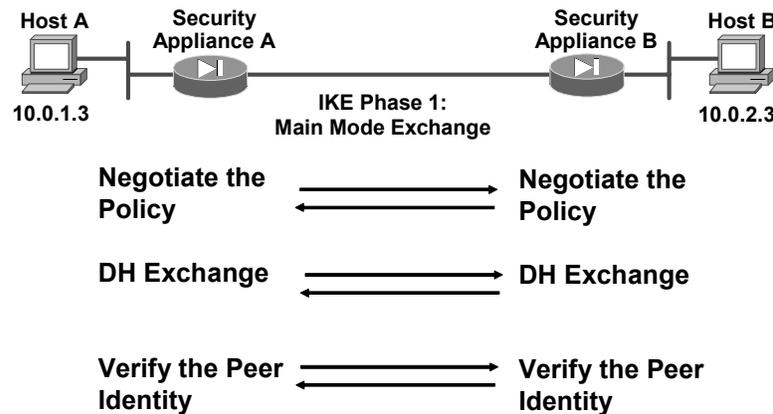
SNPA v4.0—11-10

The basic purpose of IKE Phase 1 is to negotiate IKE policy sets, authenticate the peers, and set up a secure channel between the peers. IKE Phase 1 occurs in two modes: main mode and aggressive mode.

■ Main mode has three two-way exchanges between the initiator and receiver:

— First exchange: The algorithms and hashes that are used to secure the IKE communications are negotiated and agreed upon between peers.

— Second exchange: This exchange uses a DH exchange to generate shared secret keys and pass nonces, which are random numbers sent to the other party, signed, and returned to prove their identity. The shared secret key is used to generate all the other encryption and authentication keys.

— Third exchange: This exchange verifies the other side's identity. It is used to authenticate the remote peer. The main outcome of main mode is a secure communication path for subsequent exchanges between the peers. Without proper authentication, you might establish a secure communication channel with a hacker who could be stealing all your sensitive material.

■ In the aggressive mode, fewer exchanges are done and with fewer packets. The first exchange covers almost all of the steps: the IKE policy set negotiation; the DH public key generation; a nonce, which the other party signs; and an identity packet, which can be used to verify the identity of the other party via a third party. The receiver sends everything back that is needed to complete the exchange. The only thing left is for the initiator to confirm the exchange.

IKE Phase 1 Policy Sets

Host A   **Security Appliance A**   **Security Appliance B**   **Host B**

10.0.1.3   Negotiate IKE Proposals   10.0.2.3

Policy Set 10
DES
MD5
Pre-share
DH1
Lifetime

IKE Policy Sets

Policy Set 15
DES
MD5
Pre-share
DH1
Lifetime

Policy Set 20
3DES
SHA
Pre-share
DH1
Lifetime

- **Negotiates matching IKE transform sets to protect IKE exchange**

        SNPA v4.0—11-11
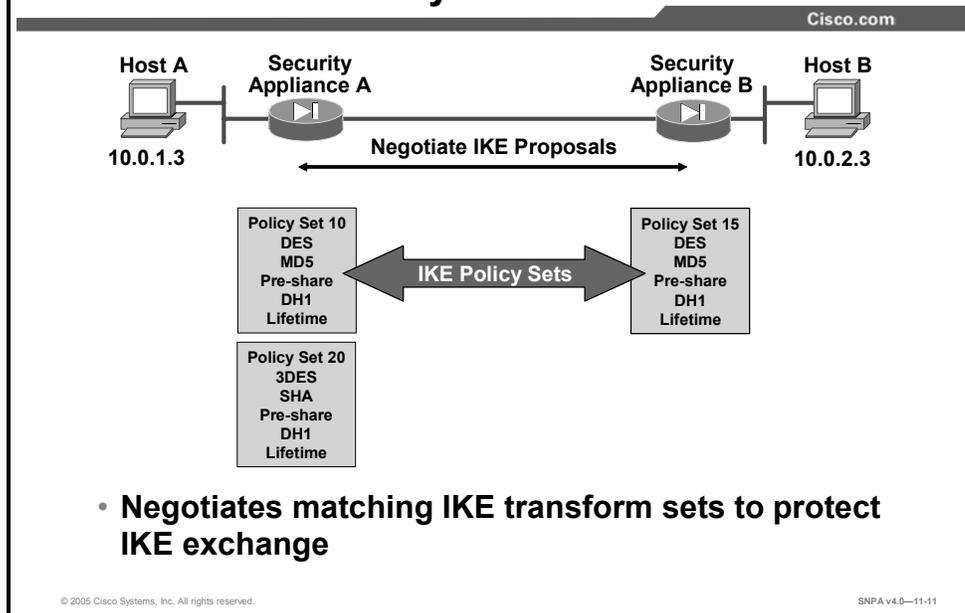
When trying to make a secure connection between hosts A and B through the Internet, IKE security proposals are exchanged between security appliances A and B. The proposals identify the crypto attributes that will be used to secure the IKE protocol exchanges. Under each proposal, the originator must delineate which algorithms are employed in the proposal (for example, DES with MD5). Rather than negotiate each algorithm individually, the algorithms are grouped into sets, called IKE transform sets. A transform set delineates which encryption algorithm, authentication algorithm, mode, and key length are proposed. These IKE proposals and transform sets are exchanged during the IKE main mode first exchange phase. If a transform set match is found between peers, the main mode continues. If no match is found, the tunnel is shut down.

In the example in the figure, security appliance A sends IKE transform sets 10 and 20 to security appliance B. Security appliance B compares its set, transform set 15, with those received from security appliance A. In this instance, there is a match: security appliance A's transform set 10 matches security appliance B's transform set 15.

In a point-to-point application, each end may only need a single IKE policy set defined. However, in a hub-and-spoke environment, the central site may require multiple IKE policy sets to satisfy all the remote peers.

DH Key Exchange

Terry
Public Key B
+ Private Key A
Shared Secret
Key (BA)

Alex
Public Key A
+ Private Key B
Shared Secret
Key (AB)

Key = Key

| Pay to Terry Smith | $100.00 |
| One Hundred and xx/100 | Dollars |

→ Encrypt

Decrypt →

| Pay to Terry Smith | $100.00 |
| One Hundred and xx/100 | Dollars |

4ehIDx67NMop9eR U78IOPotVBn45TR → **Internet** → 4ehIDx67NMop9eR U78IOPotVBn45TR

SNPA v4.0—11-12
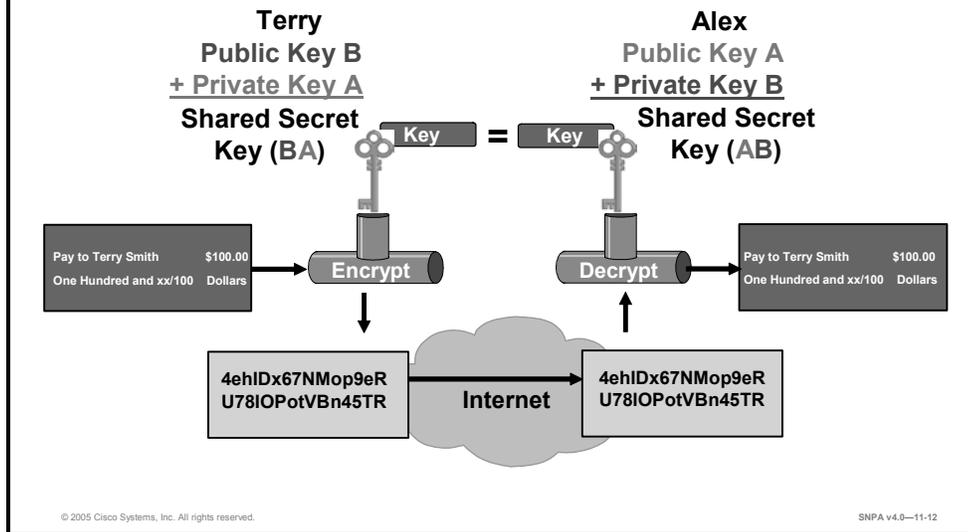
DH key exchange is a public key exchange method that provides a way for two peers to establish a shared secret key over an insecure communication path. With DH, there are several different DH algorithms or groups defined, DH groups 1−7. A group number defines an algorithm and unique values. For instance, group 1 defines a prime modular exponential (MODP) algorithm with a 768-bit prime number. Group 2 defines an MODP algorithm with a 1024-bit prime number. During IKE Phase 1, the group is negotiated between peers. Between Cisco VPN devices, groups 1, 2, 5, and 7 are supported.

After the group negotiations are completed, the shared secret key is calculated. The shared secret key, SKEYID, is used in the derivation of three other keys: SKEYID_a, SKEYID_d, and SKEYID_e. Each key has a separate purpose. SKEYID_a is the keying material used during the authentication process. SKEYID_d is the keying material used to derive keys for non-ISAKMP SAs. SKEYID_e is the keying material used in the encryption process. All four keys are calculated during IKE Phase 1.

Authenticate Peer Identity
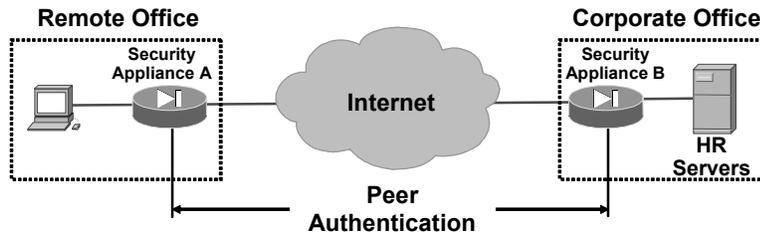
Remote Office

Security Appliance A

Internet

Corporate Office

Security Appliance B

HR Servers

Peer Authentication

Peer authentication methods

- **Pre-shared keys**
- **RSA Signature**
- **DSA Signature**

SNPA v4.0—11-13

When conducting business over the Internet, you must know who is at the other end of the tunnel. The device on the other end of the VPN tunnel must be authenticated before the communications path is considered secure. The last exchange of IKE Phase 1 is used to authenticate the remote peer.

The security appliance supports two data origin authentication methods:

- Pre-shared keys: A secret key value entered for each peer is manually used to authenticate the peer

- RSA Signature: Specifies RSA Signature as the authentication method

- DSA Signature: Specifies DSA Signature as the authentication method

Step 3: IKE Phase 2

Host A

Security Appliance A

Security Appliance B

Host B

10.0.1.3

Negotiate IPSec Security Parameters

10.0.2.3

SNPA v4.0—11-14

The purpose of IKE Phase 2 is to negotiate the IPSec security parameters that are used to secure the IPSec tunnel. IKE Phase 2 performs the following functions:

■ Negotiates IPSec security parameters and IPSec transform sets

■ Establishes IPSec SAs

■ Periodically renegotiates IPSec SAs to ensure security

■ (Optional) Performs an additional DH exchange

IKE Phase 2 has one mode, called quick mode. Quick mode occurs after IKE has established the secure tunnel in Phase 1. It negotiates a shared IPSec transform, derives shared secret keying material used for the IPSec security algorithms, and establishes IPSec SAs. Quick mode exchanges nonces that are used to generate new shared secret key material and prevent replay attacks from generating bogus SAs.

Quick mode is also used to renegotiate a new IPSec SA when the IPSec SA lifetime expires. And quick mode refreshes the keying material that is used to create the shared secret key that is based on the keying material derived from the DH exchange in Phase 1.

IPSec Transform Sets

Host A   **Security Appliance A**   **Security Appliance B**   **Host B**

10.0.1.3   ← **Negotiate Transform Sets** →   10.0.2.3

Transform Set 30   **Transform Set 55**
ESP   ESP
3DES   3DES
SHA   ← **IPSec transform sets** →   SHA
Tunnel   Tunnel
Lifetime   Lifetime

Transform Set 40
ESP
DES   • **A transform set is a combination**
MD5   **of algorithms and protocols that**
Tunnel   **enacts a security policy for traffic.**
Lifetime
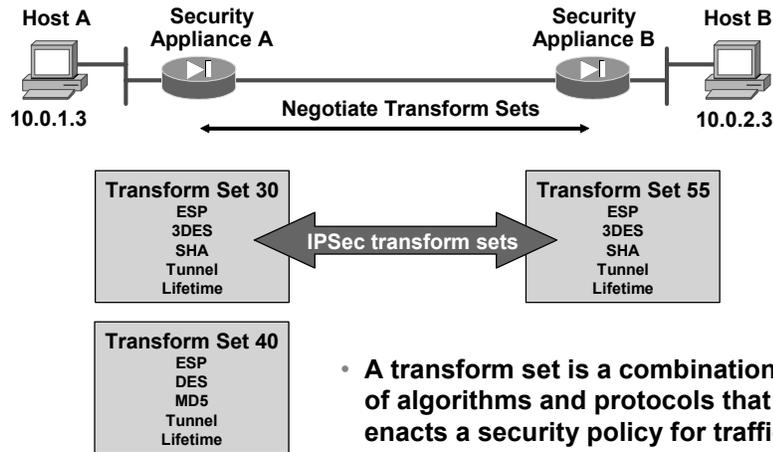
SNPA v4.0—11-15

The ultimate goal of IKE Phase 2 is to establish a secure IPSec session between endpoints. Before that can happen, each pair of endpoints negotiates the level of security required (for example, encryption and authentication algorithms for the session). Rather than negotiate each protocol individually, the protocols are grouped into sets, called IPSec transform sets. IPSec transform sets are exchanged between peers during quick mode. If a match is found between sets, IPSec session-establishment continues. If no match is found, the session is halted.

In the example in the figure, security appliance A sends IPSec transform sets 30 and 40 to security appliance B. Security appliance B compares its set, transform set 55, with those received from security appliance A. In this instance, there is a match. Security appliance A's transform set 30 matches security appliance B's transform set 55. These encryption and authentication algorithms form an SA.
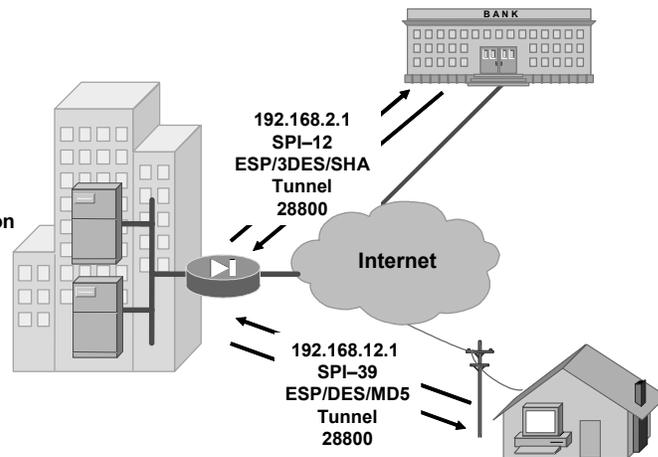
SNPA v4.0—11-16

When the security services are agreed upon between peers, each VPN peer device enters the information in a security policy database (SPD). The information includes the encryption and authentication algorithm, destination IP address, transport mode, key lifetime, and so on. This information is referred to as the SA. An SA is a one-way logical connection that provides security to all traffic traversing the connection. Because most traffic is bidirectional, two SAs are required: one for inbound traffic and one for outbound traffic. The VPN device indexes the SA with a number, a security parameter index (SPI). Rather than send the individual parameters of the SA across the tunnel, the source gateway, or host, inserts the SPI into the ESP header. When the IPSec peer receives the packet, it looks up the destination IP address, IPSec protocol, and SPI in its SA database (SAD), then processes the packet according to the algorithms listed under the SPD.

The IPSec SA is a compilation of the SAD and the SPD. The SAD is used to identify the SA destination IP address, IPSec protocol, and SPI number. The SPD defines the security services applied to the SA, encryption and authentication algorithms, and mode and key lifetime. For example, in the corporate-to-bank connection, the security policy provides a very secure tunnel using 3DES, SHA, tunnel mode, and a key lifetime of 28800. The SAD value is 192.168.1.1, ESP, and SPI-12. For the remote user accessing e-mail, a less secure policy is negotiated using DES, MD5, tunnel mode, and a key lifetime of 28800. The SAD values are a destination IP address of 192.168.6.1, ESP, and SPI-39.

SA Lifetime

Data-Based   Time-Based

SNPA v4.0—11-17

The longer you keep a password on your company PC, the more vulnerable it becomes. The same is true of keys and SAs. For good security, the SA and keys should be changed periodically. There are two parameters to consider: lifetime type and duration. The first parameter, lifetime type, defines how the lifetime is measured, by the number of bytes transmitted or the amount of time transpired. The second parameter, the duration, is expressed in either kilobytes of data or seconds of time. For example, you might specify a lifetime based on 10,000 kilobytes of data transmitted or 28,800 seconds of time expired. The keys and SAs remain active until their lifetime expires or until some external event—the client drops the tunnel—causes them to be deleted.

Step 4: IPSec Session

Host A   Security Appliance A   Security Appliance B   Host B

IPSec Session
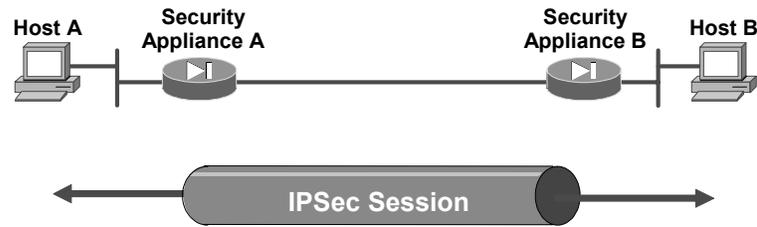
- **SAs are exchanged between peers.**
- **The negotiated security services are applied to the traffic.**

SNPA v4.0—11-18

After IKE Phase 2 is complete and quick mode has established IPSec SAs, traffic is exchanged between hosts A and B via a secure tunnel. Interesting traffic is encrypted and decrypted according to the security services specified in the IPSec SA.

Step 5: Tunnel Termination

Host A   **Security Appliance A**   **Security Appliance B**   **Host B**
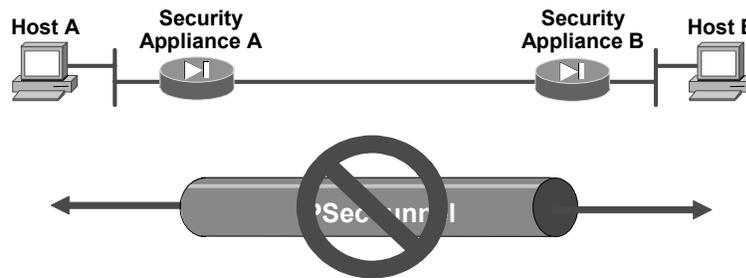
IPSec tunnel

- **A tunnel is terminated:**
  - **By an SA lifetime timeout**
  - **If the packet counter is exceeded**
- **Removes IPSec SA**

SNPA v4.0—11-19

IPSec SAs terminate through deletion or by timing out. An SA can time out when a specified number of seconds has elapsed or when a specified number of bytes has passed through the tunnel. When the SAs terminate, the keys are also discarded. When subsequent IPSec SAs are needed for a flow, IKE performs a new Phase 2 negotiation and, if necessary, a new Phase 1 negotiation. A successful negotiation results in new SAs and new keys. New SAs are usually established before the existing SAs expire so that a given flow can continue uninterrupted.

Configure VPN Connection Parameters

This topic provides an overview of configuring VPN connection parameters on the security appliance.

tunnel-group Command

- **To create and manage the database of connection-specific records for IPSec, use the** tunnel-group **command in global configuration mode.**
- **The** tunnel-group **command has the following subcommands:**
  - tunnel-group general-attributes
  - tunnel-group ipsec-attributes

firewall(config)#

```
tunnel-group name type type
```

```
fw1(config)# tunnel-group training type ipsec-l2l
```

SNPA v4.0—11-21

You configure a tunnel group to identify authentication, authorization, and accounting (AAA) servers, specify connection parameters, and define a default group policy. The security appliance stores tunnel groups internally. There are two default tunnel groups in the security appliance system: DefaultRAGroup, which is the default IPSec remote-access tunnel group, and DefaultL2Lgroup, which is the default IPSec LAN-to-LAN tunnel group. You can change them, but you cannot delete them. The security appliance uses these groups to configure default tunnel parameters for remote access and LAN-to-LAN tunnel groups when there is no specific tunnel group identified during tunnel negotiation.

Each of these **tunnel-group** commands puts you in a configuration mode for configuring various attributes of the tunnel group.

- **tunnel-group general-attributes**—This mode is used to configure settings that are common to all supported tunneling protocols.

- **tunnel-group ipsec-attributes**—This mode is used to configure settings that are specific to the IPSec tunneling protocol.

The syntax for this command is as follows:

tunnel-group *name* **type** *type*

name	Specifies the name of the tunnel group. This can be any string you choose. If the name is an IP address, it is usually the IP address of the peer.
type	Specifies the type of tunnel group: ■ **ipsec-ra**—IPSec remote access ■ **ipsec-l2l**—IPSec LAN-to-LAN

tunnel-group general-attributes Command

- **The general-attribute sub-configuration mode is used to configure settings that are common to all supported tunneling protocols.**
- **The tunnel-group general-attributes command has the following subcommands:**
  - accounting-server-group
  - address-pool
  - authentication-server-group
  - authorization-server-group
  - default-group-policy
  - dhcp-server
  - strip-group
  - strip-realm

firewall(config)#

```
tunnel-group name general-attributes
```

```
fw1(config)# tunnel-group training general
fw1(config-general)#
```

SNPA v4.0—11-22

The general-attribute configuration mode is used to configure settings that are common to all supported tunneling protocols.

The following subcommands are available:

- **accounting-server-group**—Specifies the AAA server group to use for user accounting

- **address-pool**—Specifies the name of the address pool that is configured with the **ip local pool** command

- **authentication-server-group**—Specifies the AAA server group to use for user authentication; default is LOCAL

- **authorization-server-group**—Specifies the AAA server group to use for user authorization

- **default-group-policy**—Specifies the set of attributes that the user inherits by default

- **dhcp-server**—Configures support for Dynamic Host Configuration Protocol (DHCP) servers that assign IP addresses to clients as a VPN tunnel is established

- **strip-group**—Enables or disables strip-group processing

- **strip-realm**—Enables or disable strip-realm processing

tunnel-group ipsec-attributes Command

- **The ipsec-attribute sub-configuration mode is used to configure settings that are specific to the IPSec tunneling protocol.**
- **The** tunnel-group ipsec-attribute **command has the following subcommands:**
    - authorization-dn-attributes
    - authorization-required
    - chain
    - client-update
    - isakmp keepalive
    - peer-id-validate
    - pre-shared-key
    - radius-with-expiry
    - trust-point

firewall(config)#

```
tunnel-group name ipsec-attributes
```

```
fw1(config)# tunnel-group training ipsec-attributes
fw1(config-ipsec)#
```

The ipsec-attribute configuration mode is used to configure settings that are specific to the IPSec tunneling protocol.

The following subcommands are available:

- **authorization-dn-attributes**—Specifies what part of the subject distinguished name (DN) field will be as the username for authorization

- **authorization-required**—Requires users to authorize successfully in order to connect

- **chain**—Enables sending a certificate chain

- **client-update**—Configures and changes client update parameters

- **isakmp keepalive**—Configures IKE dead peer detection (DPD)

- **peer-id-validate**—Specifies whether to validate the identity of the peer using the peer's certificate

- **pre-shared-key**—Specifies a pre-shared key to support IKE connections that is based on pre-shared keys.

- **radius-with-expiry**—Has the security appliance use Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) v2 to negotiate a password update with the user during authentication

- **trust-point**—Specifies the name of a trustpoint that identifies the certificate that is to be sent to the IKE peer

IPSec Configuration Tasks

This topic describes the tasks you perform when configuring an IPSec-based VPN.

Configuring IPSec Encryption

- **Task 1: Prepare to configure VPN support.**
- **Task 2: Configure IKE parameters.**
- **Task 3: Configure IPSec parameters.**
- **Task 4: Test and verify VPN configuration.**

SNPA v4.0—11-25

The rest of this lesson demonstrates how to configure an IPSec-based VPN between two security appliances operating as secure gateways, using pre-shared keys for authentication. The four tasks that you must perform to configure IPSec encryption on the security appliance are summarized here.

- Task 1: Prepare to configure VPN support. This task consists of several steps that determine IPSec policies, ensure that the network works, and ensure that the security appliance can support IPSec.

- Task 2: Configure IKE parameters. This task consists of several configuration steps that ensure that IKE can set up secure channels to desired IPSec peers. IKE can set up IPSec SAs, enabling IPSec sessions. IKE negotiates IKE parameters and sets up IKE SAs during an IKE Phase 1 exchange called main mode.

- Task 3: Configure IPSec parameters. This task consists of several configuration steps that specify IPSec SA parameters between peers and set global IPSec values. IKE negotiates SA parameters and sets up IPSec SAs during an IKE Phase 2 exchange called quick mode.

- Task 4: Test and verify VPN configuration. After you configure IPSec, you will need to verify that you have configured it correctly and to ensure that it works.

Task 1: Prepare to Configure VPN Support

Successful implementation of an IPSec network requires preparation in advance of beginning the configuration of individual security appliances. This topic outlines how to determine network design details.

Task 1: Prepare for IKE and IPSec

Cisco.com

- **Step 1: Determine the IKE (IKE Phase 1) policy.**
- **Step 2: Determine the IPSec (IKE Phase 2) policy.**
- **Step 3: Ensure that the network works without encryption.**
- **Step 4: (Optional) Implicitly permit IPSec packets to bypass security appliance ACLs and access groups.**

SNPA v4.0—11-27

Configuring IPSec encryption can be complicated. You must plan in advance if you want to configure IPSec encryption correctly the first time and minimize misconfiguration. You should begin this task by defining the overall security needs and strategy based on the overall company security policy. Some planning steps include the following:

Step 87   Determine the IKE (IKE Phase 1) policy: Determine the IKE policies between peers based on the number and location of IPSec peers.

Step 88   Determine the IPSec (IKE Phase 2) policy: Identify IPSec peer details, such as IP addresses and IPSec modes. Determine the IPSec policies that are applied to the encrypted data passing between peers.

Step 89   Ensure that the network works without encryption: Ensure that basic connectivity has been achieved between IPSec peers using the desired IP services before configuring security appliance IPSec.

Step 90   Implicitly permit IPSec packets to bypass security appliance access control lists (ACLs), access groups, and conduits: In this step, you enter the **sysopt connection permit-ipsec** command (on by default).

Determine IKE Phase 1 Policy

Parameter	Strong	Stronger
Encryption algorithm	DES	3DES or AES
Hash algorithm	MD5	SHA-1
Authentication method	Pre-share	RSA Signature
Key exchange	DH Group 1	DH Group 2 or 5
IKE SA lifetime	86,400 seconds	< 86,400 seconds

SNPA v4.0—11-28

An IKE policy defines a combination of security parameters to be used during the IKE negotiation. A group of policies makes up a protection suite of multiple policies that enable IPSec peers to establish IKE sessions and SAs with a minimum of configuration.

Create IKE Policies for a Purpose

IKE negotiations must be protected, so each IKE negotiation begins by each peer agreeing on a common (shared) IKE policy. This policy states which security parameters will be used to protect subsequent IKE negotiations.

After the two peers agree upon a policy, an SA established at each peer identifies the security parameters of the policy. These SAs apply to all subsequent IKE traffic during the negotiation.

You can create multiple, prioritized policies at each peer to ensure that at least one policy will match a remote peer's policy.

Define IKE Policy Parameters

You can select specific values for each IKE parameter, per the IKE standard. You choose one value over another based on the security level you desire and the type of IPSec peer to which you will connect.

There are five parameters to define in each IKE policy, as outlined in the previous figure and in the following table. The figure shows the relative strength of each parameter, and the table shows the default values.

IKE Policy Parameters

Parameter	Accepted Values	Keyword	Default
Message encryption algorithm	56-bit DES 168-bit 3DES AES 128-bit key AES 192-bit key AES 256-bit key	**des** **3des** **aes** **aes-192** **aes-256**	DES
Message integrity (hash) algorithm	SHA-1 (HMAC variant) MD5 (HMAC variant)	**sha** **md5**	SHA-1
Peer authentication method	Pre-shared keys RSA Signature DSA Signature	**pre-share** **rsa-sig** **dsa-sig**	RSA Signature
Key exchange parameters (DH group ID)	768-bit DH 1024-bit DH 1536-bit DH Elliptical curve field size: 163 bits	**1** **2** **5** **7**	768-bit DH
ISAKMP-established SA lifetime	Can specify any number of seconds	—	86,400 seconds (1 day)

Note 3DES provides stronger encryption than DES. AES provides stronger security than DES and is computationally more efficient than 3DES. 3DES may be restricted for export or import into some countries.

Determine IPSec (IKE Phase 2) Policy

Cisco.com

Site 1
10.0.1.11

Security
Appliance 1
e0 192.168.1.2

Internet

Security
Appliance 6
e0 192.168.6.2
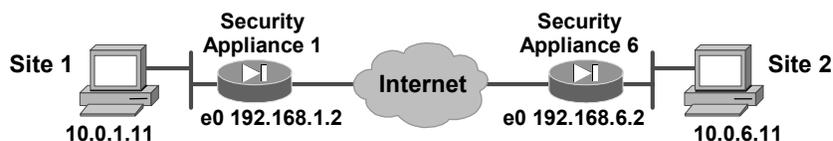
Site 2
10.0.6.11

Policy	Site 1	Site 2
Transform set	ESP-DES, tunnel	ESP-DES, tunnel
Peer security appliance IP address	192.168.1.2	192.168.6.2
Encrypting hosts	10.0.1.11	10.0.6.11
Traffic (packet type) to be encrypted	IP	IP

SNPA v4.0—11-29

Determining network design details includes defining a more detailed security policy for protecting traffic. You can then use the detailed policy to help select IPSec transform sets and modes of operation. Your security policy should answer the following questions:

- What protections are required or are acceptable for the protected traffic?
- What traffic should or should not be protected?
- Which security appliance interfaces are involved in protecting internal networks, external networks, or both?
- What are the peer IPSec endpoints for the traffic?

The figure shows a summary of IPSec encryption policy details that will be configured in upcoming examples.

Task 2: Configure IKE Parameters

The next major task in configuring security appliance IPSec is to configure the IKE parameters gathered in the previous task. This topic presents the steps used to configure IKE policies.

Task 2: Configure IKE

Cisco.com

- **Step 1: Enable or disable IKE.**
- **Step 2: Configure IKE Phase 1 policy.**
- **Step 3: Configure a tunnel group.**
- **Step 4: Configure the tunnel group attributes pre-shared key.**
- **Step 5: Verify IKE Phase 1 policy.**

SNPA v4.0—11-31

Configuring IKE consists of the following essential steps:

Step 91   Enable or disable IKE.

Step 92   Configure an IKE Phase 1 policy.

Step 93   Configure a tunnel group.

Step 94   Configure the tunnel group attributes pre-shared key.

Step 95   Verify IKE Phase 1 policy.

Enable or Disable IKE

Site 1 10.0.1.11 — **Security Appliance 1** e0 192.168.1.2 — **Internet** — e0 192.168.6.2 **Security Appliance 6** — **Site 2** 10.0.6.11
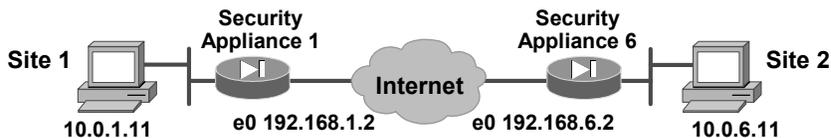
firewall(config)#

```
isakmp enable interface-name
```

- **Enables or disables IKE on the security appliance interfaces**
- **Disables IKE on interfaces not used for IPSec**

```
fw1(config)# isakmp enable outside
```

SNPA v4.0—11-32

Step 96 Enable or disable IKE (ISAKMP):

```
firewall(config)# isakmp enable interface-name
```

interface-name	Specifies the name of the interface on which to enable or disable ISAKMP negotiation

Specify the security appliance interface on which the IPSec peer will communicate. IKE is enabled by default and for individual security appliance interfaces. Use the **no isakmp enable** *interface-name* command to disable IKE.

Configure IKE Phase 1 Policy

Security Appliance 1

Security Appliance 6

Site 1

Internet

Site 2

10.0.1.11   e0 192.168.1.2   e0 192.168.6.2   10.0.6.11

```
fw1(config)# isakmp policy 10 encryption des
fw1(config)# isakmp policy 10 hash sha
fw1(config)# isakmp policy 10 authentication pre-share
fw1(config)# isakmp policy 10 group 1
fw1(config)# isakmp policy 10 lifetime 86400
```

- **Creates a policy suite grouped by priority number**
- **Creates policy suites that match peers**
- **Can use default values**

SNPA v4.0—11-33

Step 97   Configure an IKE Phase 1 policy with the **isakmp policy** command to match expected IPSec peers by completing the following substeps:

16. Identify the policy with a unique priority designation, according to the table.

firewall(config)# isakmp policy *priority*

aes	Specifies that encrypted IKE messages protected by this suite are encrypted using AES with a 128-bit key.
aes-192	Specifies that encrypted IKE messages protected by this suite are encrypted using AES with a 192-bit key.
aes-256	Specifies that encrypted IKE messages protected by this suite are encrypted using AES with a 256-bit key.
des	Specifies 56-bit DES cipher block chaining (CBC) as the encryption algorithm that is to be used in the IKE policy.
3des	Specifies that the 3DES encryption algorithm is to be used in the IKE policy.
group 1	Specifies that the 768-bit DH group 1 is to be used in the IKE policy. This is the default value.
group 2	Specifies that the 1024-bit DH group 2 is to be used in the IKE policy.
group 5	Specifies that the 1536-bit DH group 5 is to be used in the IKE policy.
group 7	Specifies that DH group 7 is to be used in the IKE policy. Group 7 generates IPSec SA keys, where the elliptical curve field size is 163 bits.
lifetime seconds	Specifies how many seconds each SA should exist before expiring. To propose a finite lifetime, use an integer from 120 to 86,400 seconds (one day). Specify 0 seconds for infinite lifetime.
md5	Specifies MD5 (HMAC variant) as the hash algorithm that is to

	be used in the IKE policy.
sha	Specifies SHA-1 (HMAC variant) as the hash algorithm that is to be used in the IKE policy. This is the default hash algorithm.
pre-share	Specifies pre-shared keys as the authentication method.
priority	Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 65534, with 1 being the highest priority and 65534 the lowest.
rsa-sig	Specifies RSA Signature as the authentication method.
	RSA Signature provides nonrepudiation for the IKE negotiation. This means that you can prove to a third party whether you had an IKE negotiation with the peer.
dsa-sig	Specifies DSA Signature as the authentication method.

17. Specify the encryption algorithm (the default is 3DES):

```
firewall(config)# isakmp policy priority encryption {aes |
aes-192| aes-256 | des | 3des}
```

18. Specify the hash algorithm (the default is **sha**):

```
firewall(config)# isakmp policy priority hash {md5 | sha}
```

19. Specify the authentication method:

```
firewall(config)# isakmp policy priority authentication {pre-
share | dsa-sig | rsa-sig}
```

If you specify the authentication method of pre-shared keys, you must manually configure these keys, which is outlined in Step 3.

20. Specify the DH group ID (the default is group 2):

```
firewall(config)# isakmp policy priority group {1 | 2 | 5 | 7}
```

21. Specify the IKE SA's lifetime (the default is 86,400):

```
firewall(config)# isakmp policy priority lifetime seconds
```

Note	Security appliance software has preset default values. If you enter a default value for a given policy parameter, it will not be written in the configuration. If you do not specify a value for a given policy parameter, the default value is assigned.

Configure a Tunnel Group
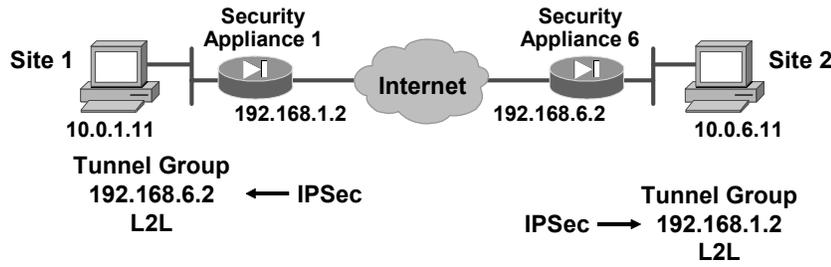
Security Appliance 1

Security Appliance 6

Site 1   **Internet**   **Site 2**

10.0.1.11   **192.168.1.2**   **192.168.6.2**   **10.0.6.11**

Tunnel Group
192.168.6.2   ← **IPSec**
L2L

IPSec → **192.168.1.2**
Tunnel Group
L2L

firewall(config)#

```
tunnel-group name type type
```

- **Names the tunnel group**
- **Defines the type of VPN connection that is to be established**

```
fw1(config)# tunnel-group 192.168.6.2 type ipsec-l2l
```

     SNPA v4.0—11-34

Step 98   Configure a tunnel group:

```
firewall(config)# tunnel-group name type type
```

name	Specifies the name of the tunnel group. This can be any string you choose. If the name is an IP address, it is usually the IP address of the peer.
type	Specifies the type of tunnel group: • **ipsec-ra**—IPSec remote access • **ipsec-l2l**—IPSec LAN-to-LAN

A tunnel group is a set of records that contain tunnel connection policies. You configure a tunnel group to identify AAA servers, specify connection parameters, and define a default group policy. The security appliance stores tunnel groups internally. There are two default tunnel groups in the security appliance system: DefaultRAGroup, which is the default IPSec remote-access tunnel group, and DefaultL2Lgroup, which is the default IPSec LAN-to-LAN tunnel group. You can change them, but you cannot delete them. The security appliance uses these groups to configure default tunnel parameters for remote access and LAN-to-LAN tunnel groups when there is no specific tunnel group identified during tunnel negotiation. To establish a basic LAN-to-LAN connection, you must set two attributes for a tunnel group:

■ Set the connection type to IPSec LAN-to-LAN.

■ Configure an authentication method, in this example, pre-shared key.

Configure Tunnel Group Attributes
Pre-Shared Key
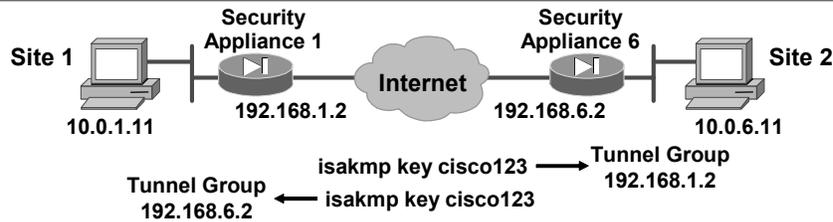
Security Appliance 1

Security Appliance 6

Site 1

Internet

Site 2

10.0.1.11

192.168.1.2

192.168.6.2

10.0.6.11

isakmp key cisco123 ⟶ **Tunnel Group 192.168.1.2**

Tunnel Group 192.168.6.2 ⟵ isakmp key cisco123

firewall(config)#

```
tunnel-group name [general-attributes | ipsec-attributes]
```

• **Enters tunnel-group ipsec-attributes subconfiguration mode**

firewall(config-ipsec)#

```
pre-shared-key key
```

• **Associates a pre-shared key with the connection policy**

```
fw1(config)# tunnel-group 192.168.6.2 ipsec-attributes
fw1(config-ipsec)# pre-shared-key cisco123
```

SNPA v4.0—11-35

Step 99   Configure the tunnel group pre-shared key attribute:

```
firewall(config)# tunnel-group name ipsec-attributes
```

name	Specifies the name of the tunnel-group.

Each of these **tunnel-group** commands puts you in a configuration mode for configuring various attributes of the tunnel group.

■ **tunnel-group general-attributes**—This mode is used to configure settings that are common to all supported tunneling protocols.

■ **tunnel-group ipsec-attributes**—This mode is used to configure settings that are specific to the IPSec tunneling protocol.

```
firewall(config-ipsec)# pre-shared-key key
```

key	Specifies a pre-shared key to support IKE connections that are based on pre-shared keys; the key is alphanumeric from one to 128 characters.

Verify IKE Phase 1 Policy

Cisco.com

Site 1 — Security Appliance 1 — Internet — Security Appliance 6 — Site 2

10.0.1.11   192.168.1.2   192.168.6.2   10.0.6.11
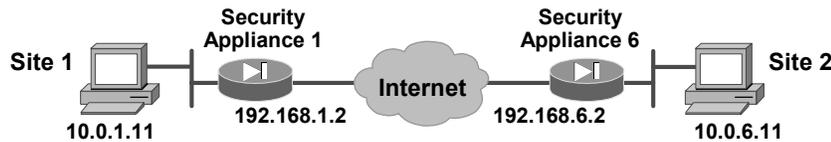
```
fw1# show run crypto isakmp
isakmp identity address
isakmp enable outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
```

- **Displays configured and default IKE protection suites**

SNPA v4.0—11-36

Step 100   Verify IKE Phase 1 policies.

The **show running-config crypto isakmp** command displays configured and default policies, as shown in the figure. The **show running-config crypto isakmp** command displays configured policies much as they would appear with the **write terminal** command, as follows:

```
fw1# show run crypto isakmp
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
```

The **show run tunnel-group** command displays tunnel group information, including attributes, about all tunnel groups or a specified tunnel group.

```
fw1# show run tunnel-group
tunnel-group 192.168.6.2 type ipsec-l2l
tunnel-group 192.168.6.2 ipsec-attributes
pre-shared-key *
```

Task 3: Configure IPSec Parameters

The next major task in configuring security appliance IPSec is to configure the previously gathered IPSec parameters. This topic presents the steps used to configure IPSec parameters for IKE pre-shared keys.

Task 3: Configure IPSec

Cisco.com

Step 1: **Configure interesting traffic: NAT 0 and ACL.**
- access-list 101 permit
- nat 0

Step 2: **Configure IPSec transform set suites.**
- crypto ipsec transform-set

Step 3: **Configure the crypto map.**
- crypto map

Step 4: **Apply the crypto map.**
- crypto map *map-name* interface *interface-name*

SNPA v4.0—11-38

The tasks and commands used to configure IPSec encryption on a security appliance are summarized here:

Step 101   Configure interesting traffic.

Step 102   Configure IPSec transform set suites.

Step 103   Configure the crypto map.

Step 104   Apply the crypto map to the interface.

Configure Interesting Traffic

Cisco.com

Site 1 — 10.0.1.11

Security Appliance 1 — 192.168.1.2

Internet

Security Appliance 6 — 192.168.6.2

Site 2 — 10.0.6.11

10.0.1.X → Encrypt

Encrypt ← 10.0.6.X
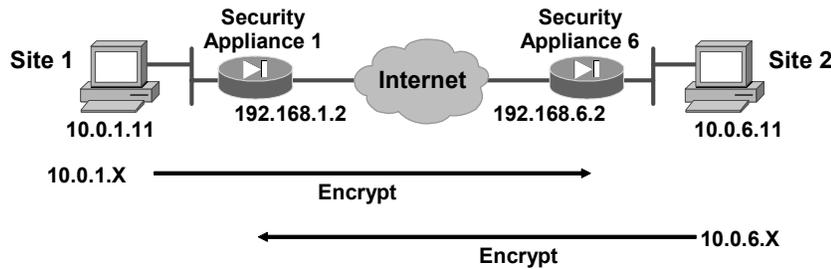
```
fw1(config)# access-list 101 permit ip 10.0.1.0
255.255.255.0 10.0.6.0 255.255.255.0
```

• permit **= encrypt**
• deny **= do not encrypt**

SNPA v4.0—11-39

Step 105   Configure a crypto ACL.

Crypto ACLs are traffic selection ACLs. They are used to define which IP traffic is interesting and will be protected by IPSec and which traffic will not be protected by IPSec. Crypto ACLs perform the following functions:

■ Indicate the data flow to be protected by IPSec

■ Select outbound traffic to be protected by IPSec

■ Process inbound traffic in order to filter out and discard traffic that should be protected by IPSec

■ Determine whether or not to accept requests for IPSec SAs for the requested data flows when processing IKE negotiations

Note   Although the ACL syntax is unchanged from the ACL that is applied to security appliance interfaces, the meanings are slightly different for crypto ACLs—**permit** specifies that matching packets must be encrypted whereas **deny** specifies that matching packets need not be encrypted.

Any unprotected inbound traffic that matches a permit entry in the ACL for a crypto map entry, flagged as IPSec, will be dropped because this traffic was expected to be protected by IPSec.

If you want certain traffic to receive one combination of IPSec protection (for example, authentication only) and other traffic to receive a different combination of IPSec protection (for example, both authentication and encryption), you must create two different crypto ACLs to define the two different types of traffic. These different ACLs are then used in different crypto map entries, which specify different IPSec policies.

.

Caution	It is recommended that you avoid using the **any** keyword to specify source or destination addresses. The **permit any any** statement is strongly discouraged because this will cause all outbound traffic to be protected (and all protected traffic to be sent to the peer, specified in the corresponding crypto map entry) and will require protection for all inbound traffic. All inbound packets that lack IPSec protection will then be silently dropped, including packets for routing protocols, Network Time Protocol (NTP), echo, echo response, and so on.

Try to be as restrictive as possible when defining which packets to protect in a crypto ACL. If you must use the **any** keyword in a permit statement, you must preface that statement with a series of deny statements to filter out traffic (that would otherwise fall within that permit statement) that you do not want protected.

Example: Crypto ACLs

Cisco.com

Site 1   Security Appliance 1   Internet   Security Appliance 6   Site 2

10.0.1.11   e0 192.168.1.2   e0 192.168.6.2   10.0.6.11

- **Lists are symmetrical.**

Security Appliance 1 (fw1)

```
fw1# show run access-list
access-list 101 permit ip 10.0.1.0 255.255.255.0 10.0.6.0
  255.255.255.0
```

Security Appliance 6 (fw6)

```
fw6# show run access-list
access-list 101 permit ip 10.0.6.0 255.255.255.0 10.0.1.0
  255.255.255.0
```

SNPA v4.0—11-40

Use the **show run access-list** command to display currently configured ACLs. The figure contains an example ACL for each of the peer security appliances. In the Security Appliance 1 ACL, the source network is 10.0.1.0 and the destination network is 10.0.6.0. In the Security Appliance 6 ACL, the source network is 10.0.6.0 and the destination address is 10.0.1.0. The ACLs are symmetrical.

Configure Interesting Traffic: NAT 0
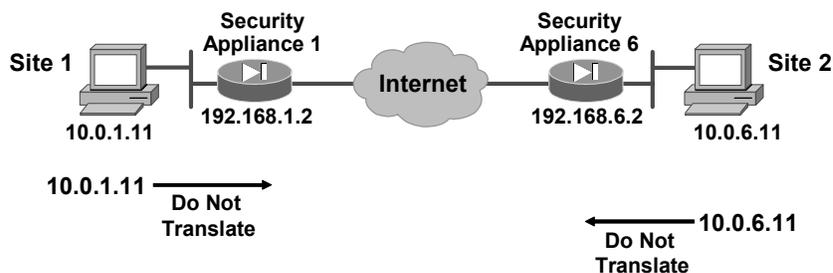
Security Appliance 1

Security Appliance 6

Site 1

Internet

Site 2

10.0.1.11

192.168.1.2

192.168.6.2

10.0.6.11

10.0.1.11 → Do Not Translate

← 10.0.6.11 Do Not Translate

```
fw1(config)# nat (inside) 0 access-list 101
```

The **nat 0** command instructs the security appliance not to use Network Address Translation (NAT) for any traffic deemed as interesting traffic for IPSec. All traffic that matches the **access-list** command statement will be exempt from NAT services. In the figure, traffic that matches ACL 101—traffic from 10.0.1.0/24 to 10.0.6.0/24—is exempt from NAT.

```
nat (real_ifc) 0 access-list access_list_name
```

access-list	Associates **access-list** command statements with the **nat 0** command and exempts from NAT processing traffic that matches the ACL.
access_list_name	The ACL name.
real_ifc	The name of the network interface, as specified by the **nameif** command, through which the hosts or network designated by *local_ip* are accessed.

Configure an IPSec Transform Set

Site 1   **Security Appliance 1**   Internet   **Security Appliance 6**   **Site 2**

10.0.1.11   e0 192.168.1.2   e0 192.168.6.2   10.0.6.11
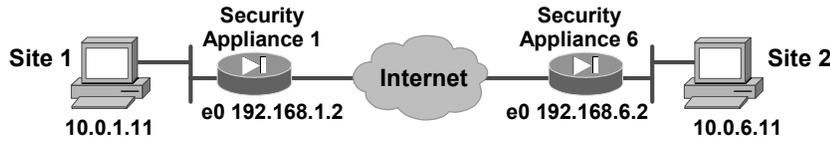
firewall(config)#

```
crypto ipsec transform-set transform-set-name
 transform1 [transform2]
```

- **Sets are limited to two transforms**

- **Default mode is tunnel**

- **Configures matching sets between IPSec peers**

```
fw1(config)# crypto ipsec transform-set fw6 esp-des
 esp-md5-hmac
```

SNPA v4.0—11-42

Step 106   Configure an IPSec transform set:

```
firewall(config)# crypto ipsec transform-set transform-set-
name transform1 [transform2]
```

transform-set-name	The name of the transform set to create or modify.
transform1 *transform2*	Specifies up to two transforms. Transforms define the IPSec security protocol(s) and algorithm(s). Each transform represents an IPSec security protocol plus the algorithm to use.

Transforms define the IPSec security protocols and algorithms. Each transform represents an IPSec security protocol plus the algorithm you want to use.

You can specify multiple transform sets, then specify one or more of these transform sets in a crypto map entry. The transform set that is defined in the crypto map entry will be used in the IPSec SA negotiation to protect the data flows specified by the ACL of that crypto map entry.

During the IPSec SA negotiation, the peers agree to use a particular transform set for protecting a particular data flow.

A transform set equals an ESP transform plus the mode (transport or tunnel). Transform sets are limited to two ESP transforms. The default mode is tunnel. Be sure to configure matching transform sets between IPSec peers.

Available IPSec Transforms

```
Security                          Security
Appliance 1                       Appliance 6
Site 1                                                              Site 2

        e0 192.168.1.2    Internet    e0 192.168.6.2
10.0.1.11                                                     10.0.6.11
```
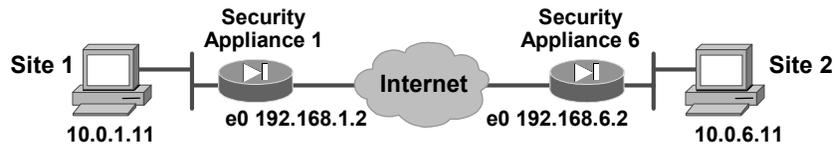
```
esp-des       ESP transform using DES cipher (56 bits)
esp-3des      ESP transform using 3DES cipher(168 bits)
esp-aes       ESP transform using AES-128 cipher
esp-aes-192   ESP transform using AES-192 cipher
esp-aes-256   ESP transform using AES-256 cipher
esp-md5-hmac  ESP transform using HMAC-MD5 auth
esp-sha-hmac  ESP transform using HMAC-SHA auth
esp-none      ESP no authentication
esp-null      ESP null encryption
```

The security appliance supports the transforms listed in the figure.

Choosing IPSec transform combinations can be complex. The following tips may help you select transforms that are appropriate for your situation:

- If you want to provide data confidentiality, include an ESP encryption transform.

- Also consider including an ESP authentication transform or an AH transform to provide authentication services for the transform set:

    — To ensure data authentication for the outer IP header as well as the data, include an AH transform.

    — To ensure data authentication, use either ESP or AH. You can choose MD5 or SHA (HMAC keyed hash variants) as your authentication algorithm.

- SHA is generally considered stronger than MD5, but it is slower.

- Examples of acceptable transform combinations are as follows:

    — esp-des for high-performance encryption

    — ah-md5-hmac for authenticating packet contents with no encryption

    — esp-3des and esp-md5-hmac for strong encryption and authentication

    — ah-sha-hmac and esp-3des and esp-sha-hmac for strong encryption and authentication

Configure the Crypto Map

Site 1 **Security Appliance 1** **Internet** **Security Appliance 6** **Site 2**

e0 192.168.1.2   e0 192.168.6.2

10.0.1.11   10.0.6.11

```
fw1(config)# crypto map FW1MAP 10 match address 101
fw1(config)# crypto map FW1MAP 10 set peer 192.168.6.2
fw1(config)# crypto map FW1MAP 10 set transform-set pix6
fw1(config)# crypto map FW1MAP 10 set security-association
  lifetime seconds 28800
```

- **Specifies IPSec (IKE Phase 2) parameters**
- **Maps names and sequence numbers of group entries into a policy**

SNPA v4.0—11-44

Step 107 Configure the crypto map with the **crypto map** command by completing the following substeps:

1. Assign an ACL to the crypto map entry:

    firewall(config)# crypto map *map-name* *seq-num* match address *acl_name*

match address	Assigns an ACL to a crypto map entry
seq-num	The number you assign to the crypto map entry
map-name	Specifies the name of the crypto map set

2. Specify the peer to which the IPSec-protected traffic can be forwarded:

    firewall(config)# crypto *map map-name* *seq-num* set peer {*ip_address* | *hostname*}{*...ip_address* | *hostname10*}

hostname	Specifies a peer by its hostname as defined by the security appliance **name** command.
set peer	Specifies an IPSec peer in a crypto map entry either by hostname or IP address.
ip_address	Specify a peer by its IP address.

This specifies the peer hostname or IP address. For LAN-to-LAN connections, you can use multiple peers only with originator-only connection type. Configuring multiple peers is equivalent to providing a fallback list. For each tunnel, the security appliance attempts to negotiate with the first peer in the list. If that peer does not respond, the security appliance works its way down the list until either a peer responds or there are no more peers in the list.

3. Specify which transform sets are allowed for this crypto map entry.

```
firewall(config)# crypto map map-name seq-num set transform-
set transform-set-name 1[... transform-set-name9]
```

set *transform-set*	Specify which transform sets can be used with the crypto map entry.
transform-set-name1 *transform-set-name9*	Specifies the name(s) of the transform set(s), defined using the **crypto ipsec transform-set** command, to use for the crypto map. For an IPSec ISAKMP or dynamic crypto map entry, you can specify up to nine transform sets.

If you use multiple transform sets, list them in order of priority (highest priority first). You can specify up to nine transform sets.

4. (Optional) Specify whether IPSec will ask for Perfect Forward Secrecy (PFS) when requesting new SAs for this crypto map entry or will require PFS in requests received from the peer:

```
firewall(config)# crypto map map-name seq-num set pfs [group1
| group2 | group5 | group7]
```

group1	Specifies that IPSec should use the 768-bit DH prime modulus group when performing the new DH exchange.
group2	Specifies the IPSec peer's IP address for the pre-shared key and that IPSec should use the 1024-bit DH prime modulus group when performing the new DH exchange.
group5	Specifies that IPSec should use the 1536-bit DH prime modulus group when performing the new DH exchange.
group7	Specifies that IPSec should use group 7 (Elliptic Curve Cryptography [ECC]) where the elliptical curve field size is 163 bits, for example, with the Movian VPN client.
set pfs	Specifies that IPSec should ask for PFS. With PFS, every time a new SA is negotiated, a new DH exchange occurs. (This exchange requires additional processing time.)

Note	PFS provides additional security for DH key exchanges at the cost of additional processing.

5. (Optional) Specify the SA lifetime for the crypto map entry if you want the SAs for this entry to be negotiated using IPSec SA lifetimes other than the global lifetimes:

```
firewall(config)# crypto map map-name seq-num set security-
association lifetime {seconds seconds | kilobytes kilobytes}
```

set security-association lifetime	Used to override (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPSec SAs.
kilobytes	Specifies the volume of traffic (in kilobytes) that can pass between peers using a given SA before it expires. The default is 4,608,000 kilobytes.
seconds	Specifies the number of seconds a security association will live before it expires. The default is 28,800 seconds (8 hours).

6. (Optional) Specify dynamic crypto maps with the **crypto dynamic-map** *dynamic-map-name dynamic-seq-num* **match address** *acl_name* command. A dynamic crypto map entry is essentially a crypto map entry without all the parameters configured. It acts as a policy template where the missing parameters are later dynamically configured (as the result of an IPSec negotiation) to match a peer's requirements. This allows peers to exchange IPSec traffic with the security appliance even if the security appliance does not have a crypto map entry specifically configured to meet all the peer's requirements.

Apply the Crypto Map to an Interface

Cisco.com

Site 1 — Security Appliance 1 — Internet — Security Appliance 6 — Site 2

10.0.1.11   e0 192.168.1.2   e0 192.168.6.2   10.0.6.11

```
firewall(config)#
```

```
crypto map map-name interface interface-name
```

• **Applies the crypto map to an interface**
• **Activates IPSec policy**

```
fw1(config)# crypto map FW1MAP interface outside
```

SNPA v4.0—11-45

Step 108   Apply the crypto map to an interface:

```
firewall(config)# crypto map map-name interface interface-name
```

interface-name	Specifies the interface for the SA to use for establishing tunnels with VPN peers. If ISAKMP is enabled and you are using a CA to obtain certificates, this should be the interface with the address specified in the CA certificates.
map-name	Specifies the name of the crypto map set.

This command applies the crypto map to an interface and activates the IPSec policy. The SA supports IPSec termination on any and all active interfaces. You must assign a crypto map set to an interface before that interface can provide IPSec services.

You can assign only one crypto map set to an interface. If multiple crypto map entries have the same *map-name* but a different *seq-num*, they are part of the same set and are all applied to the interface. The security appliance evaluates the crypto map entry that has the lowest *seq-num* first.

Example: Crypto Map for Security Appliance 1
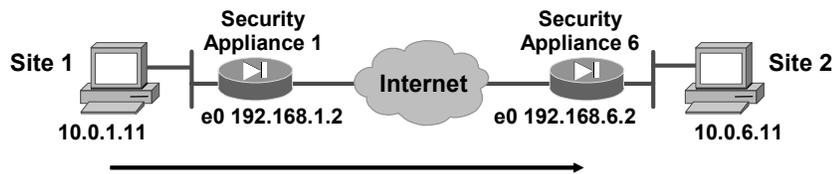
Security Appliance 1 (fw1)

```
fw1# show run crypto map
crypto map FW1MAP 10 match address 101
crypto map FW1MAP 10 set peer 192.168.6.2
crypto map FW1MAP 10 set transform-set pix6
crypto map FW1MAP interface outside
```

SNPA v4.0—11-46

Use the **show run crypto map** command to verify the crypto map configuration. The figure shows an example of a crypto map for Security Appliance 1.

Example: Crypto Map for Security Appliance 6

Cisco.com

Site 1   **Security Appliance 1**   **Internet**   **Security Appliance 6**   **Site 2**

10.0.1.11   e0 192.168.1.2   e0 192.168.6.2   10.0.6.11
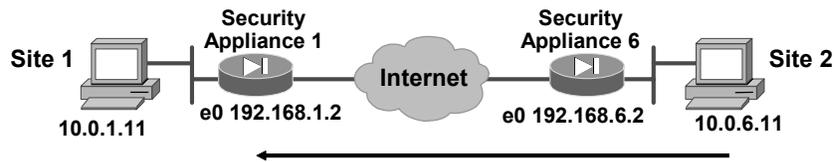
Security Appliance 1 (fw6)

```
fw6# show run crypto map
crypto map FW1MAP 10 match address 101
crypto map FW1MAP 10 set peer 192.168.1.2
crypto map FW1MAP 10 set transform-set pix1
crypto map FW1MAP interface outside
```

SNPA v4.0—11-47

This figure shows an example of a crypto map for Security Appliance 6.

Task 4: Test and Verify VPN Configuration

The last major task in configuring security appliance IPSec is to test and verify the IKE and IPSec configurations you accomplished in the previous tasks. This topic presents the methods and commands that are used to test and verify VPN configuration.

Task 4: Test and Verify VPN Configuration

- **Verify ACLs and interesting traffic.**
  – show run access-list
- **Verify correct IKE configuration.**
  – show run isakmp
  – show run tunnel-group
- **Verify correct IPSec configuration.**
  – show run ipsec

SNPA v4.0—11-49

You can perform the following actions to test and verify that you have correctly configured the VPN on the security appliance:

■   Verify ACLs and select interesting traffic with the **show run access-list** command.

■   Verify correct IKE configuration with the **show run isakmp** and **show run tunnel-group** commands.

■   Verify correct IPSec configuration of transform sets with the **show run ipsec** command.

Task 4: Test and Verify VPN Configuration (Cont.)

- **Verify correct crypto map configuration.**
  - show run crypto map
- **Clear IPSec SA.**
  - clear crypto ipsec sa
- **Clear IKE SA.**
  - clear crypto isakmp sa
- **Debug IKE and IPSec traffic through the security appliance.**
  - debug crypto ipsec
  - debug crypto isakmp

SNPA v4.0—11-50

You also can perform these actions to test and verify that you have correctly configured the VPN on the security appliance:

- Verify the correct crypto map configuration with the **show run crypto map** command.

- Clear IPSec SAs for testing of SA establishment with the **clear crypto ipsec sa** command.

- Clear IKE SAs for testing of IKE SA establishment with the **clear crypto isakmp sa** command.

- Debug IKE and IPSec traffic through the security appliance with the **debug crypto ipsec** and **debug crypto isakmp** commands.

Scale Security Appliance VPNs

This topic explains how to scale security appliance VPNs using CAs.

SNPA v4.0—11-52
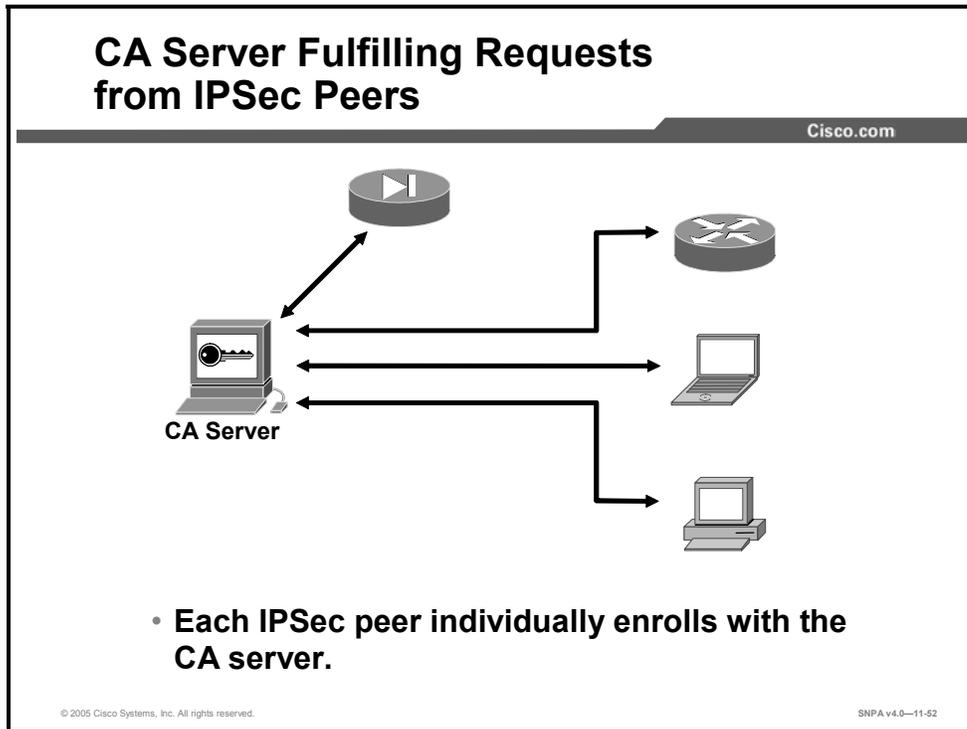
The use of pre-shared keys for IKE authentication works only when you have a few IPSec peers. CAs enable scaling to a large number of IPSec peers. Although there are a number of scaling methods, using a CA server is the most scalable solution. Other IKE authentication methods require manual intervention to generate and distribute the keys on a per-peer basis. The CA server enrollment process can be largely automated so that it scales well to large deployments. Each IPSec peer individually enrolls with the CA server and obtains public and private encryption keys compatible with other peers enrolled with the server.

Enroll a Security Appliance with a CA

CA Server

- **The security appliance generates public and private key pair.**
- **The security appliance obtains public key and certificate from the CA.**
- **The security appliance requests signed certificate from the CA.**
- **The CA administrator verifies request and sends signed certificate.**

Peers enroll with a CA server in a series of steps in which specific keys are generated and then exchanged by the security appliance and the CA server to ultimately form a signed certificate. The enrollment steps can be summarized as follows:

Step 109 The security appliance generates an RSA public and private key pair.

Step 110 The security appliance obtains a public key and its certificate from the CA server.

Step 111 The security appliance requests a signed certificate from the CA using the generated RSA keys and the public key certificate from the CA server.

Step 112 The CA administrator verifies the request and sends a signed certificate.

Summary

This topic summarizes what you learned in this lesson.

Summary

- **A VPN is a service that offers secure, reliable connectivity over a shared public network infrastructure such as the Internet.**
- **Cisco security appliances enable a secure VPN.**
- **IPSec configuration tasks include configuring IKE and IPSec parameters.**
- **CAs enable scaling to a large number of IPSec peers.**

SNPA v4.0—11-54

Lesson 12

Configuring Security Appliance Remote Access Using Cisco Easy VPN

Overview

This lesson begins with a discussion of Cisco Easy Virtual Private Network, its two components, and its modes of operation, then continues with an overview of the Cisco VPN Client. The lesson then details how Cisco Easy VPN works and how it is configured.
The lesson concludes with information regarding the installation and configuration of the Cisco VPN Client.

Objectives

Upon completing this lesson, you will be able to describe the general functions of firewalls and security appliances in regards to secure remote access. This includes being able to meet these objectives:

- Describe the Easy VPN Server
- Describe the Easy VPN Remote
- Configure the Easy VPN Server
- Configure the Easy VPN Remote using the Cisco VPN Client

Introduction to Cisco Easy VPN

This topic discusses Cisco Easy VPN, its two components and modes of operation.
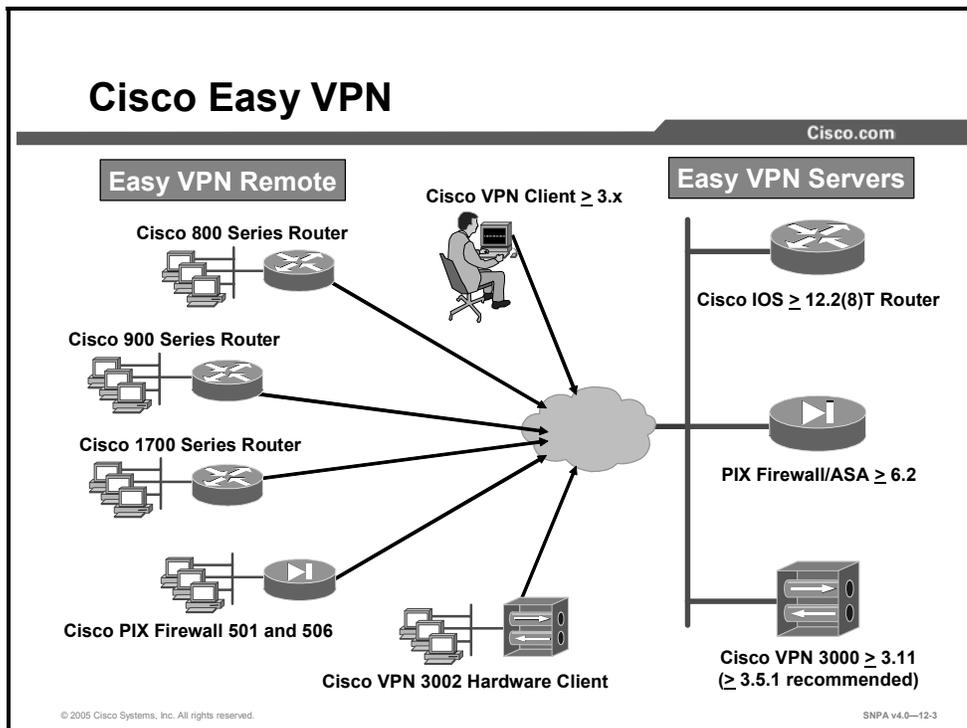
Cisco Easy VPN, a software enhancement for existing security appliances, greatly simplifies VPN deployment for remote offices and teleworkers. Based on the Cisco Unified Client framework, Cisco Easy VPN centralizes VPN management across all Cisco VPN devices, greatly reducing the complexity of VPN deployments. Easy VPN enables an integration of Easy VPN Remotes—Cisco routers, Cisco security appliances, the Cisco VPN 3002 Hardware and Software Clients—within a single deployment with a consistent policy and key management method that greatly simplifies remote side administration.

Cisco Easy VPN consists of two components: the Cisco Easy VPN Server and the Cisco Easy VPN Remote feature.

Features of Cisco Easy VPN Server

- **Server support for Cisco Easy VPN Remote Clients was introduced with the release of the Cisco PIX Firewall Software v6.2.**
- **It allows remote end users to communicate using IPSec with supported security appliance VPN gateways.**
- **Centrally managed IPSec policies are pushed to the clients by the server, minimizing configuration by the end users.**

SNPA v4.0—12-4

The Easy VPN Server enables Cisco IOS routers, security appliances, and Cisco VPN 3000 Series Concentrators to act as VPN headend devices in site-to-site or remote access VPNs, where the remote office devices are using the Easy VPN Remote feature. Using this feature, security policies defined at the headend are pushed to the remote VPN device, insuring that those connections have up-to-date policies in place before the connection is established.

In addition, an Easy VPN Server-enabled device can terminate IPSec tunnels initiated by mobile remote workers who are running Cisco VPN Client software on PCs. This flexibility makes it possible for mobile and remote workers, such as salespeople on the road or teleworkers, to access their company's intranet, where critical data and applications exist.

The security appliance Cisco Easy VPN Server introduces server support for the Cisco Easy VPN Remote Clients. It allows remote end users to communicate using IPSec with supported Cisco VPN gateways. Centrally managed IPSec policies are pushed to the clients by the server, minimizing configuration by the end users.

Supported Easy VPN Servers

Cisco.com

Easy VPN Servers

Cisco VPN Client ≥ 3.x

Cisco 800 Series Router

Cisco 900 Series Router

Cisco 1700 Series Router

Cisco PIX Firewall 501 and 506

Cisco VPN 3002 Hardware Client

Cisco IOS ≥ 12.2(8)T router

PIX Firewall/ASA ≥ 6.2

Cisco VPN 3000 ≥ 3.11
(≥ 3.5.1 recommended)

SNPA v4.0—12-5
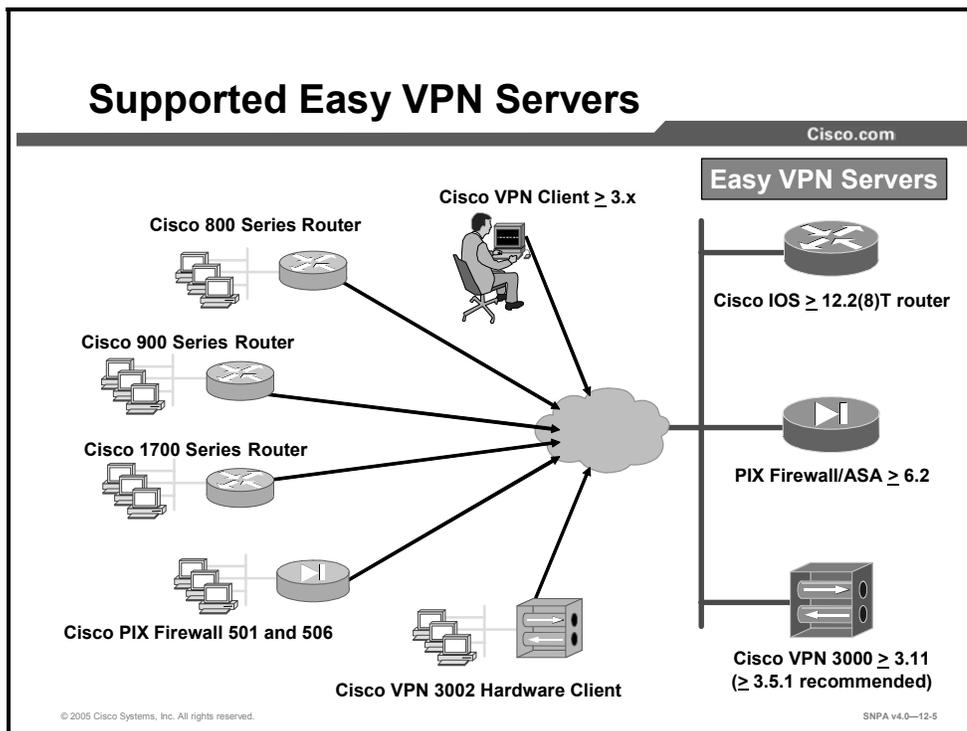
The Easy VPN Remote feature requires that the destination peer be a VPN gateway or concentrator that supports the Easy VPN Server. This includes the following platforms when running the indicated software releases:

■ Cisco 806, Cisco 826, Cisco 827, and Cisco 828 Routers: Cisco IOS Software Release 12.2(8)T or later release

■ Cisco 1700 Series Routers: Cisco IOS Software Release 12.2(8)T or later release

■ Cisco 2600 Series Routers: Cisco IOS Software Release 12.2(8)T or later release

■ Cisco 3620 Router: Cisco IOS Software Release 12.2(8)T or later release

■ Cisco 3640 Routes: Cisco IOS Software Release 12.2(8)T or later release

■ Cisco 3660 Router: Cisco IOS Software Release 12.2(8)T or later release

■ Cisco 7100 Series VPN Routers: Cisco IOS Software Release 12.2(8)T or later release

■ Cisco 7200 Router: Cisco IOS Software Release 12.2(8)T or later release

■ Cisco 7500 Series Routers: Cisco IOS Software Release 12.2(8)T or later release

■ Cisco uBR905 and Cisco uBR925 Cable Access Routers: Cisco IOS Software Release 12.2(8)T or later release

■ Cisco VPN 3000 Series Concentrator: Software Release 3.11 or later release

■ Cisco PIX 500 Series Security Appliances: Cisco PIX Security Appliance Software v6.2 or later version

See Cisco.com for the latest listing of Cisco Easy VPN Remote devices and software clients.

Supported Easy VPN Remote Clients

- **Cisco VPN Software Client > 3.x**
- **Cisco VPN 3002 Hardware Client > 3.x**
- **Cisco PIX Firewall 501 and 506 VPN Client > 6.2**
- **Cisco Easy VPN Remote Router Clients**
  - **Cisco 800 Series**
  - **Cisco 900 Series**
  - **Cisco 1700 Series**

SNPA v4.0—12-6

The Easy VPN Remote feature enables Cisco IOS routers, security appliances, and Cisco VPN 3002 Hardware Clients and Software Clients to act as remote VPN Clients. As such, these devices can receive security policies from an Easy VPN Server, minimizing VPN configuration requirements at the remote location. This cost-effective solution is ideal for remote offices with little IT support or large customer premises equipment (CPE) deployments where it is impractical to individually configure multiple remote devices. This feature makes VPN configuration as easy as entering a password, which increases productivity and lowers costs as the need for local IT support is minimized.

See Cisco.com for a complete list of Cisco routers that support the Cisco Easy VPN. The following list details the Cisco VPN Clients that support the Easy VPN Remote feature:

- Cisco VPN Software Client v3.x or later
- Cisco VPN 3002 Hardware Client v3.x or later
- Cisco PIX 501/506/506E VPN Client v6.2 or later
- Cisco VPN Easy VPN Remote Routers
  - Cisco 800 Series
  - Cisco 900 Series
  - Cisco 1700 Series

See Cisco.com for the latest listing of Cisco Easy VPN Remote devices and software clients.

Easy VPN Remote Modes of Operation

Easy VPN Remote supports two modes of operation:

- **Client mode**
  - **Specifies that NAT and PAT be used.**
  - **Client automatically configures the NAT and PAT translations and the ACLs that are needed to implement the VPN tunnel.**
  - **Supports split tunneling.**
- **Network extension mode**
  - **Specifies that the hosts at the client end of the VPN connection use fully routable IP addresses.**
  - **PAT is not used.**
  - **Supports split tunneling.**

The Easy VPN Remote feature supports two modes of operation:

- Client mode: Specifies that Network Address Translation (NAT) and port address translation (PAT) be configured to allow PCs and hosts on the client side of the VPN connection to form a private network that does not use any IP addresses in the address space of the destination server. In client mode, the Easy VPN Remote feature automatically configures the NAT and PAT translation and access control lists (ACLs) that are needed to implement the VPN connection. These configurations are automatically created when the VPN connection is initiated. When the tunnel is torn down, the NAT, PAT translations and the ACL configurations are automatically deleted.

Note	The NAT and PAT translation and ACL configurations that are created by the Easy VPN Remote feature are not written to either the startup configuration or running configuration files. These configurations, however, can be displayed in Cisco routers using the **show ip nat statistics** and **show access-list** commands or in the Cisco PIX Security Appliance software (v6.2 or later) using the **show vpnclient detail** command.

- Network extension mode: Specifies that the PCs and other hosts at the client end of the IPSec tunnel be given IP addresses that are fully routable and reachable by the destination network over the tunneled network so that they form one logical network. PAT is not used, which allows the client PCs and hosts to have direct access to the PCs and hosts on the destination network.

Both modes of operation also optionally support split tunneling, which allows secure access to corporate resources through the IPSec tunnel while also allowing Internet access through a connection to an ISP or other service—thereby eliminating the corporate network from the path for web access.

Easy VPN Remote Client Mode

Cisco.com

PAT

192.168.1.2   192.168.1.1 | 10.0.1.2   VPN Tunnel   10.0.0.0/24

192.168.1.3

PIX Firewall 501/506
(Easy VPN Remote)

PIX Firewall 525
(Easy VPN Server)
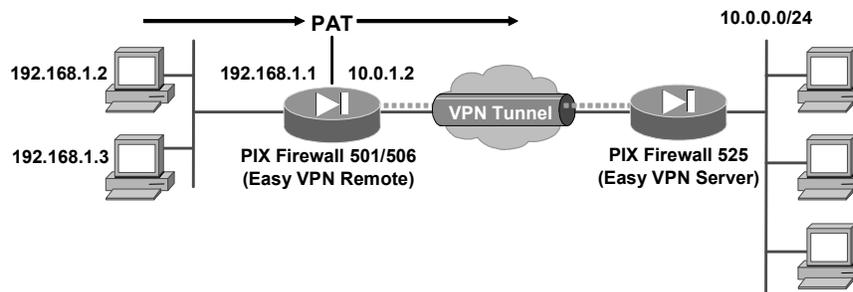
SNPA v4.0—12-8

Client mode is for those who want to deploy a VPN quickly and easily in a small office/home office (SOHO). If there is no need to see the devices behind the VPN Hardware Client and ease of use and installation is key, then client mode should be implemented. In client mode, the VPN Hardware Client uses PAT to isolate its private network from the public network. SOHO PCs behind the VPN Hardware Client are invisible to the outside network. PAT causes all traffic from the SOHO PCs to appear on the private network as a single-source IP address. The figure illustrates the Easy VPN Remote client mode of operation. In this example, the PIX 501 Security Appliance provides access to two PCs, which have IP addresses in the 192.168.1.0 private network space. These PCs connect to the Ethernet interface on the PIX 501 Security Appliance. In this example, the two PC IP addresses are translated to the PIX 501 Security Appliances outside IP address 10.0.1.2. The PIX 501 Security Appliance performs NAT and PAT translation over the IPSec tunnel so that the PCs can access the destination network.

This figure can also represent a split tunneling connection, in which the client PCs can access public resources in the Internet without including the corporate network in the path for the public resources.

Easy VPN Remote Network Extension Mode
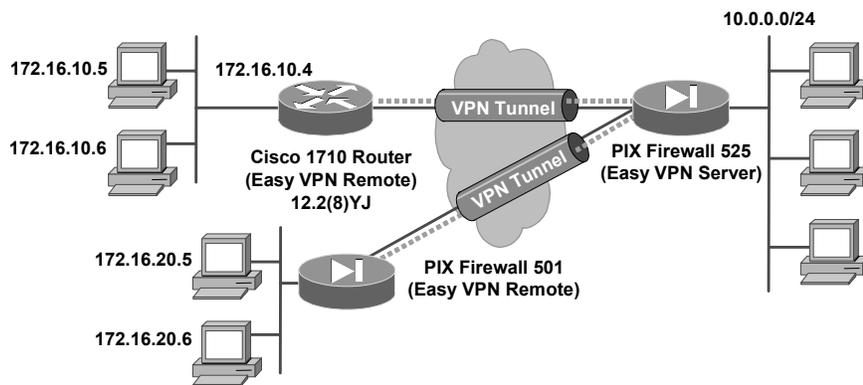
In network extension mode, all SOHO PCs on the VPN Hardware Client are uniquely addressable via the tunnel. This allows direct connection to devices behind the VPN Hardware Client. It enables central-site management information system (MIS) personnel to directly address devices behind the VPN Hardware Client over the IPSec tunnel. The figure illustrates the network extension mode of operation. In this example, the PIX 501 Security Appliance and the Cisco 1700 Series Router both act as Cisco Easy VPN Remote clients, connecting to a PIX 525 Security Appliance Easy VPN Server.

The client hosts are given IP addresses that are fully routable by the destination network over the tunnel. These IP addresses could be either in the same subnet space as the destination network, or they could be in separate subnets, as long as the destination routers are configured to properly route those IP addresses over the tunnel. This provides a seamless extension of the remote network.

Overview of Cisco VPN Client

This topic introduces you to the Cisco VPN Client, software that enables customers to establish secure, end-to-end encrypted tunnels to any Easy VPN Server. This thin design, which is an IPSec-compliant implementation, is available via Cisco.com for customers with SMARTnet support and is included free of charge with the Cisco VPN 3000 Series Concentrator.
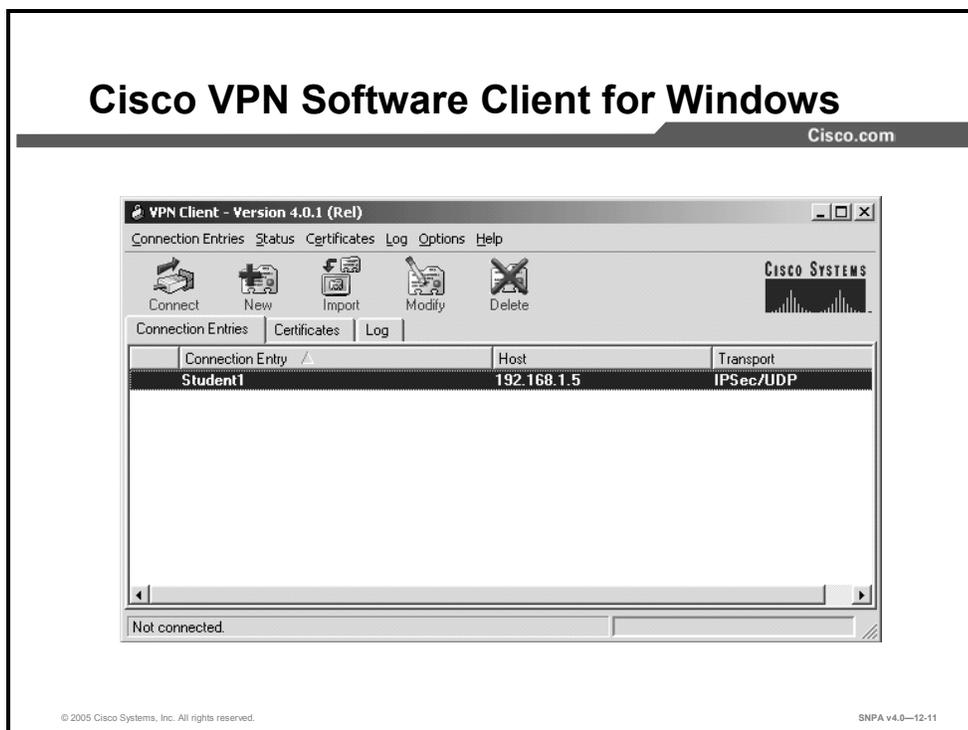
This figure displays the Cisco VPN Client splash window. Users can preconfigure the connection entry (name of connection) and hostname or IP address of remote Easy VPN Servers. Clicking **Connect** initiates Internet Key Exchange (IKE) Phase 1.

The Cisco VPN Client can be preconfigured for mass deployments, and initial logins require very little user intervention. VPN access policies and configurations are downloaded from the Easy VPN Server and pushed to the Cisco VPN Client when a connection is established, allowing simple deployment and management.

The Cisco VPN Client provides support for the following operating systems:

- Windows 95, 98, ME, NT 4.0, 2000, and XP

- Linux (Intel)

- Solaris (UltraSPARC-32 and -64 bit)

- MAC OS X 10.1

The Cisco VPN Client is compatible with the following Cisco products (Easy VPN Servers):

- Cisco IOS software-based platforms release 12.2(8)T and later

- Cisco VPN 3000 Series Concentrator v3.0 and later

- Cisco PIX Security Appliance Software v6.0 and later

Cisco VPN Client Features and Benefits

Cisco VPN Client provides the following features and benefits:

- **Intelligent peer availability detection**
- **SCEP**
- **Data compression (LZS)**
- **Command-line options for connecting, disconnecting, and connection status**
- **Configuration file with option locking**
- **Support for Microsoft network login (all platforms)**
- **DNS, WINS, and IP address assignment**
- **Load balancing and backup server support**
- **Centrally controlled policies**
- **Integrated personal firewall (stateful firewall): Zone Labs technology (Windows only)**
- **Personal firewall enforcement: Zone Alarm, BlackICE (Windows only)**

SNPA v4.0—12-12

The Cisco VPN Client provides the following features and benefits:

- Intelligent peer availability detection

- Simple Certificate Enrollment Protocol (SCEP)

- Data compression (Lempel-Ziv Compression [LZS])

- Command-line options for connecting, disconnecting, and connection status

- Configuration file with option locking

- Support for Microsoft network login (all platforms)

- Domain Name System (DNS), Windows Internet Name Service (WINS), and IP address assignment

- Load balancing and backup server support

- Centrally controlled policies

- Integrated personal firewall (stateful firewall): Zone Labs technology (Windows only)

- Personal firewall enforcement: Zone Alarm, BlackICE (Windows only)

Please note that the Cisco VPN Client supports more features than the Easy VPN Server can accommodate. Always compare the Cisco VPN Client specifications against the Easy VPN Server supported and unsupported features lists.

The specifications for the Cisco VPN Client product are as follows:

■ Supported tunneling protocols:

— IPSec Encapsulating Security Payload (ESP)

— Transparent tunneling:

■ IPSec over TCP (NAT or PAT)

■ IPSec over User Datagram Protocol (UDP) (NAT, PAT, or a firewall)

■ Supported encryption and authentication: IPSec (ESP) using Data Encryption Standard (DES), Triple DES (3DES) (56/168-bit), and Advanced Encryption Standard (AES) (128/256-bit) with Message Digest 5 (MD5) or Secure Hash Algorithm (SHA)

■ Supported key management techniques

— IKE: Aggressive and main mode (digital certificates)

— Diffie-Hellman (DH) groups 1, 2, 5, and 7

■ Supported data compression technique: LZS

■ Digital certificate support includes the following:

— Two supported enrollment mechanisms

■ SCEP

■ Certificates enrolled with Microsoft Internet Explorer

- — The supported Certificate Authorities (CAs)
  - Cisco
  - Entrust
  - GTE Cybertrust
  - Netscape
  - Baltimore
  - Rivest, Shamir, and Adleman (RSA) Keon
  - VeriSign
  - Microsoft
- — Support is provided for the Entrust Entelligence Client
- — Smartcards: Supported via Microsoft crypto application programming interface (API) (CRYPT_NOHASHOID), including the following:
  - ActivCard (Schlumberger cards)
  - eAladdin
  - Gemplus
  - Datakey
- Authentication methodologies include the following:
- — Xauth
- — RADIUS with support for:
  - State:Or reply-message attributes (token cards)
  - Security Dynamics (RSA SecurID-ready)
  - Microsoft NT Domain authentication
  - Microsoft Challenge Handshake Authentication Protocol version 2 (MSCHAPv2): NT password expiration
  - X.509 version 3 digital certificates
- Profile management: The Cisco VPN Client can be easily distributed with preconfigured Profile Configuration Files (PCFs)
- Policy management: Internet Security Association and Key Management Protocol (ISAKMP)
  - — Keeps track of centrally controlled policies, such as the following:
    - DNS information
    - WINS information
    - IP address
    - Default domain name
  - — Has the ability to save connection attributes

How Cisco Easy VPN Works

When an Easy VPN Remote Client initiates a connection with an Easy VPN Server gateway, the "conversation" that occurs between the peers generally consists of the following major steps:

■ Device authentication via IKE

■ User authentication using IKE Xauth

■ VPN policy push (using mode configuration)

■ IPSec security association (SA) creation

Easy VPN Remote Connection Process

Cisco.com

- **Step 1: The VPN Client initiates the IKE Phase 1 process.**
- **Step 2: The VPN Client negotiates an IKE SA.**
- **Step 3: The Easy VPN Server accepts the SA proposal.**
- **Step 4: The Easy VPN Server initiates a username/password challenge.**
- **Step 5: The mode configuration process is initiated.**
- **Step 6: IKE quick mode completes the connection.**

SNPA v4.0—12-15

The following is a detailed description of the Easy VPN Remote connection process:

Step 113 The Cisco VPN Client initiates the IKE Phase 1 process. The Cisco VPN Client negotiates an IKE SA.

Step 115 The Easy VPN Server accepts the SA proposal.

Step 116 The Easy VPN Server initiates a username/password challenge.

Step 117 The mode configuration process is initiated.

Step 118 IKE quick mode completes the connection.

Step 1: Cisco VPN Client Initiates IKE Phase 1 Process

Remote PC with Easy VPN Remote Client

Security Appliance Easy VPN Server

- **Using pre-shared keys? Initiate AM.**
- **Using digital certificates? Initiate MM.**

Because there are two ways to perform authentication, the Cisco VPN Client must consider the following when initiating this phase:

- If a pre-shared key is to be used for authentication, the Cisco VPN Client initiates aggressive mode (AM). When pre-shared keys are used, the accompanying group name that is entered in the configuration GUI (ID_KEY_ID) is used to identify the group profile associated with this Cisco VPN Client.

- If digital certificates are to be used for authentication, the Cisco VPN Client initiates main mode (MM). When digital certificates are used, the Organizational Unit (OU) field of a distinguished name (DN) is used to identify the group profile.

Step 2: Cisco VPN Client Negotiates an IKE SA

Remote PC with Easy VPN Remote Client

Proposal 1, Proposal 2, Proposal 3

Security Appliance Easy VPN Server

- **The Cisco VPN Client attempts to establish an SA between peer IP addresses by sending multiple IKE proposals to the Easy VPN Server.**
- **To reduce manual configuration on the VPN Client, these IKE proposals include several combinations of the following:**
  - **Encryption and hash algorithms**
  - **Authentication methods**
  - **DH group sizes**

SNPA v4.0—12-17

To reduce the amount of manual configuration on the Cisco VPN Client, a fixed combination of encryption, hash algorithms, authentication methods, and DH group sizes is proposed.

Step 3: Easy VPN Server Accepts SA Proposal

Remote PC with Easy VPN Remote Client

Security Appliance Easy VPN Server

Proposal 1

Proposal checking finds proposal 1 match.

- **The Easy VPN Server searches for a match:**
  - **The first proposal to match the server's list is accepted (highest priority match).**
  - **The most secure proposals are always listed at the top of the Easy VPN Server's proposal list (highest priority).**
- **IKE SA is successfully established.**
- **Device authentication ends and user authentication begins.**

SNPA v4.0—12-18

IKE policy is global for the Easy VPN Server and can consist of several proposals. In the case of multiple proposals, the Easy VPN Server will use the first match (so you should always have your most secure policies listed first).

Device authentication ends and user authentication begins at this point.

Step 4: Easy VPN Server Initiates a Username/Password Challenge

Cisco.com

Remote PC with Easy VPN Remote Client

Security Appliance Easy VPN Server

Username/Password Challenge

Username/Password

AAA checking

- **If the Easy VPN Server is configured for Xauth, the VPN Client waits for a username/password challenge:**
  - **The user enters a username/password combination.**
  - **The username/password information is checked against authentication entities.**
- **All Easy VPN Servers should be configured to enforce user authentication.**

SNPA v4.0—12-19

The information that is entered is checked against authentication entities using authentication, authorization, and accounting (AAA) protocols such as RADIUS and Terminal Access Controller Access Control System Plus (TACACS+). Token cards may also be used via AAA proxy.

VPN devices that are configured to handle remote Cisco VPN Clients should always be configured to enforce user authentication.

Step 5: Mode Configuration Process Is Initiated

**Remote PC with
Easy VPN
Remote Client**

**Security Appliance
Easy VPN Server**

Client Requests Parameters

**System Parameters via
Mode Configuration**

- **If the Easy VPN Server indicates successful authentication, the VPN Client requests the remaining configuration parameters from the Easy VPN Server:**
  - **Mode configuration starts.**
  - **The remaining system parameters (IP address, DNS, split tunneling information, and so on) are downloaded to the VPN Client.**
- **Remember that the IP address is the only required parameter in a group profile; all other parameters are optional.**

SNPA v4.0—12-20

The remaining system parameters (IP address, DNS, split tunnel attributes, and so on) are pushed to the Cisco VPN Client at this time using mode configuration. The IP address is the only required parameter in a group profile; all other parameters are optional.

Step 6: IKE Quick Mode Completes Connection

Remote PC with Easy VPN Remote Client

Quick Mode IPSec SA Establishment

Security Appliance Easy VPN Server

VPN Tunnel

- **After the configuration parameters have been successfully received by the VPN Client, IKE quick mode is initiated to negotiate IPSec SA establishment.**
- **After IPSec SA establishment, the VPN connection is complete.**

SNPA v4.0—12-21

After IPSec SAs are created, the connection is complete.

Configuring Users and Groups

This topic provides an overview of configuring users and groups.

Group Policy

Push to Client

Engineering Policy
Marketing Policy
Training Policy

Engineering

Marketing

Training

Internet

10.0.0.0 /24

Eng

Mktg

10.0.1.0/24

SNPA v4.0—12-23
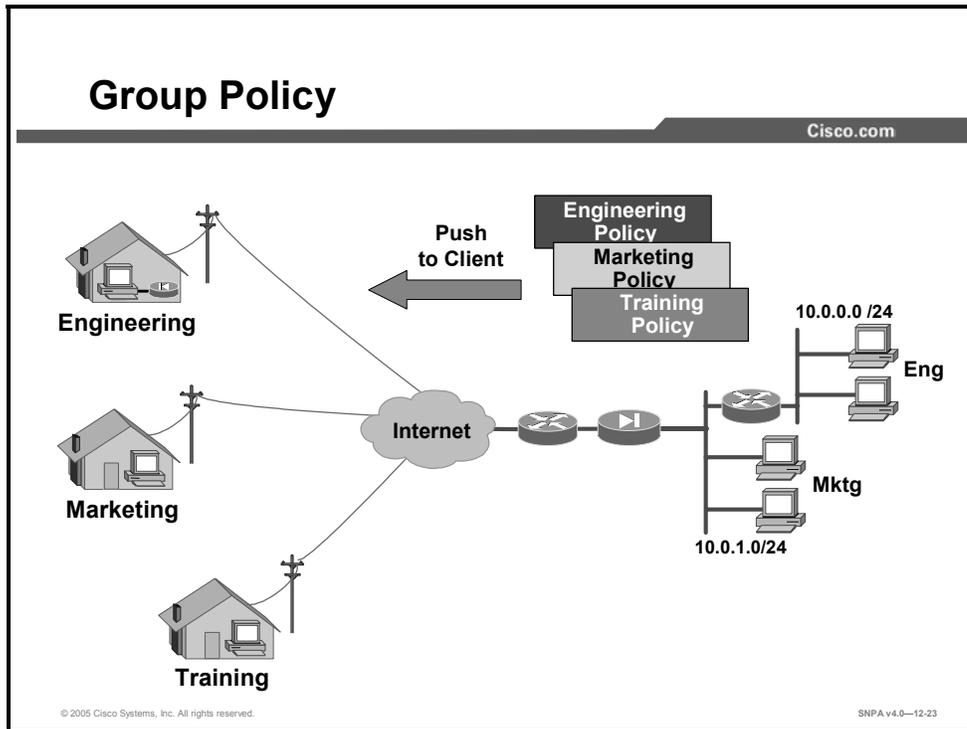
Each remote VPN user belongs to a specific VPN group. As users establish VPN tunnels to the Easy VPN Server, they identify which group they belong to. The Easy VPN Server responds by pushing the appropriate VPN group policy to the remote user. In the figure, there are three VPN group policies configured, Engineering, Marketing, and Training. Each VPN client belongs to one group. As they establish VPN tunnels, they identify which VPN group they belong to. The central site security appliance pushes a specific policy to each remote user.

Groups and Users

Base Group:
Corporate

Groups:
Departments

Users:
Individuals

MIS
/Base/Sales

VP of
MIS

Customer Service
/Base/Service

Finance
/Base/Finance

VP of
Finance
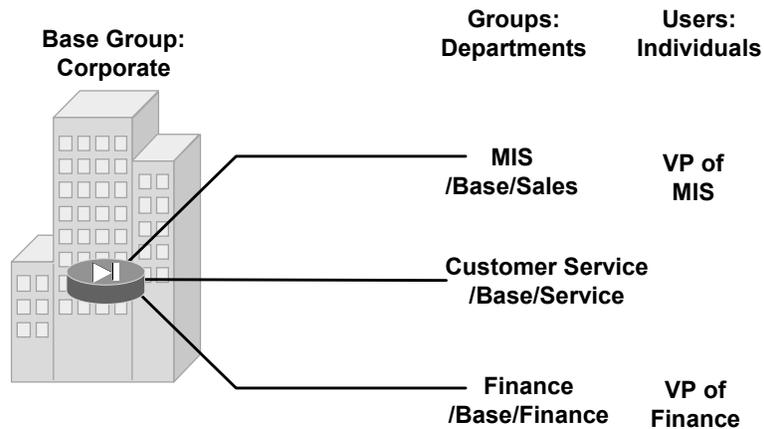
SNPA v4.0—12-24

Within a corporation, not everyone has the same access requirements: customer service engineers may require seven-day, 24-hour access; sales entry personnel need five-day, eight-hour access, and contract help might need access from 9 a.m. to 5 p.m., with restricted server access. The security appliance can accommodate different access and usage requirements. You can define different rights and privileges on a group basis. A customer service engineer, sales entry person, and contractor can be assigned to different groups. Within each group, you can configure different access hours, access protocols, idle timeouts, and server restrictions.

Within the security appliance, there are three group categories:

- Default group—The default group is a default template. The majority of the corporation access rights and privileges are defined in this group.

- Groups—Individual groups inherit the attributes of the default group, and you can then customize rights and privileges to meet the needs of specific groups.

- Users—An individual user may require a unique set of privileges.

By configuring the default group first, individual groups second, and users third, you can quickly manage access and usage rights for large numbers of users.

- **To create or edit a group policy, use the** group-policy **command in global configuration mode.**
- **A default group policy, named DfltGrpPolicy, always exists on the security appliance.**

firewall(config)#

```
group-policy {name internal [from group-policy name]}
```

```
fw1(config)# group-policy training internal
```

A default group policy, named DfltGrpPolicy, always exists on the security appliance.

The syntax for this command is as follows:

```
group-policy {name internal [from group-policy name]}
group-policy {name external server-group server group password
server password}
```

external server-group *server group*	Specifies the group policy as external and identifies the AAA server group for the security appliance to query for attributes
from *group-policy name*	Initializes the attributes of this internal group policy to the values of a preexisting group policy
internal	Identifies the group policy as internal
name	Specifies the name of the group policy
password *server password*	Provides the password to use when retrieving attributes from the external AAA server group

---

The DfltGrpPolicy has these values:

Attribute	Default Value
wins-server	none
dns-server	none
vpn-access-hours	unrestricted
vpn-simultaneous-logins	3
vpn-idle-timeout	30 minutes
vpn-session-timeout	none
vpn-filter	none
ip-comp	disable
re-xauth	disable
group-lock	none
pfs	disable
client-access-rules	none
banner	none
password-storage	disabled
ipsec-udp	disabled
ipsec-udp-port	10000
backup-servers	keep-client-config
split-tunnel-policy	tunnelall
split-tunnel-network-list	none
default-domain	none
split-dns	none
client-firewall	none
secure-unit-authentication	disabled
user-authentication	disabled
user-authentication-idle-timeout	none
ip-phone-bypass	disabled
leap-bypass	disabled
nem	disabled

group-policy attributes Command

Cisco.com

- **Use the** group-policy attributes **command in global configuration mode to enter the group-policy attributes submode.**

firewall(config)#

```
group-policy {name} attributes
```

```
fw1(config)# group-policy training attributes
fw1(config-group-policy)#
```

SNPA v4.0—12-26

You can modify the group policy attributes by entering the attributes subcommand mode, then entering the commands to modify the desired policy for the group.

The syntax for this command is as follows:

```
group-policy {name} attributes
```

name	Specifies the name of the group policy.

The following extensive list of attributes can be configured:

- **wins-server**—Sets the IP address of the primary and secondary WINS servers
- **dns-server**—Sets the IP address of the primary and secondary DNS servers
- **vpn-access-hours**—Associates a group policy with a configured time-range policy
- **vpn-simultaneous-logins**—Configures the number of simultaneous logins that are permitted for a user
- **vpn-idle-timeout**—Configures a user timeout period
- **vpn-session-timeout**—Configures a maximum amount of time for VPN connections
- **vpn-filter**—Specifies the name of the ACL to use for VPN connections
- **vpn-tunnel-protocol**—Configures a VPN tunnel type (IPSec or WebVPN)
- **ip-comp**—Enables LZS IP compression
- **re-xauth**—Requires that users reauthenticate on IKE rekey
- **group-lock**—Restricts remote users to access through the tunnel group only
- **pfs**—Enables PFS

- **client-access-rules**—Configures rules that limit the remote access client types and versions that can connect via IPSec
- **banner**—Displays a banner, or welcome text, on remote clients when they connect
- **password-storage**—Let users store their login passwords on the client system
- **ipsec-udp**—Enables IPSec over UDP
- **ipsec-udp-port**—Sets a UDP port number for IPSec over UDP
- **backup-servers**—Configures backup servers
- **split-tunnel-policy**—Sets a split tunneling policy
- **split-tunnel-network-list**—Creates a network list for split tunneling
- **default-domain**—Sets a default domain name for users of the group policy
- **split-dns**—Enters a list of domains to be resolved through the split tunnel
- **intercept-dhcp**—Enables Dynamic Host Configuration Protocol (DHCP) Intercept
- **client-firewall**—Sets personal firewall policies that the security appliance pushes to the VPN Client during IKE tunnel negotiation
- **secure-unit-authentication**—Enables secure unit authentication
- **user-authentication**—Enables user authentication
- **user-authentication-idle-timeout**—Sets an idle timeout for individual users behind hardware clients
- **ip-phone-bypass**—Enables IP Phone Bypass
- **leap-bypass**—Enables Light Extensible Authentication Protocol (LEAP) Bypass
- **nem**—Enables network extension mode for hardware clients

Users and User Attributes

- **To add a user to the security appliance database, enter the** username **command in global configuration mode.**

firewall(config)#

```
username {name} {nopassword | password password
[encrypted]} [privilege priv_level]}
```

firewall(config)#

```
username {name} attributes
```

```
fw1(config)# username user1 password 12345678
fw1(config)# username user1 attributes
fw1(config-username)#
```

SNPA v4.0—12-27

To enter the username attributes mode, use the **username attributes** command in username configuration mode. To remove all attributes for a particular user, use the **no** form of this command and append the username. To remove all attributes for all users, use the **no** form of this command without appending a username. The attributes mode lets you configure attribute-value pairs (AVPs) for a specified user. To specify the name of the group policy from which this user inherits attributes, use the **vpn-group-policy** *group-policy-name* command. Most of the same subcommand modes that are available for the group are available at the user level.

Configuring the Easy VPN Server for Extended Authentication

This topic examines the general tasks for configuring an Easy VPN Server to support Xauth for Cisco VPN Remote Client access.

Easy VPN Server General Configuration Tasks

The following general tasks are used to configure an Easy VPN Server on a security appliance:

- **Task 1: Create ISAKMP policy for remote VPN Client access.**
- **Task 2: Create IP address pool.**
- **Task 3: Define group policy for mode configuration push.**
- **Task 4: Create transform set.**
- **Task 5: Create dynamic crypto map.**
- **Task 6: Assign dynamic crypto map to static crypto map.**
- **Task 7: Apply crypto map to security appliance interface.**
- **Task 8: Configure Xauth.**
- **Task 9: Configure NAT and NAT 0.**
- **Task 10: Enable IKE DPD.**

SNPA v4.0—12-29

Complete the following tasks to configure an Easy VPN Server for Xauth with Easy VPN Remote Clients.

Task 1: Create an ISAKMP policy for remote Cisco VPN Client access.

Task 2: Create an IP address pool.

Task 3: Define a group policy for a mode configuration push.

Task 4: Create a transform set.

Task 5: Create a dynamic crypto map.

Task 6: Assign a dynamic crypto map to a static crypto map.

Task 7: Apply a dynamic crypto map to the security appliance interface.

Task 8: Configure Xauth.

Task 9: Configure NAT and NAT 0.

Task 10: Enable IKE dead peer detection (DPD).

Task 1: Create ISAKMP Policy for Remote VPN Client Access

Complete this task to configure the ISAKMP policy for an Easy VPN Server. Use the standard ISAKMP configuration commands to accomplish this task. Here is a general example of how to configure the ISAKMP policy. Start in global configuration mode:
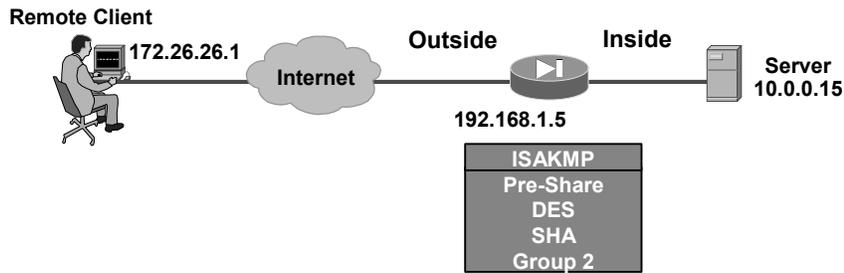
```
fw1(config)# isakmp enable outside
fw1(config)# isakmp policy 20 authen pre-share
fw1(config)# isakmp policy 20 encryption 3des
fw1(config)# isakmp policy 20 hash sha
fw1(config)# isakmp policy 20 group 2
```

The syntax for these commands is as follows:

```
isakmp policy priority authentication {pre-share | dsa-sig |
rsa-sig}
isakmp policy priority encryption {aes | aes-192| aes-256 |
des | 3des}
isakmp policy priority group {1 | 2 | 5 |7}
isakmp policy priority hash md5 | sha
isakmp policy priority lifetime seconds
```

aes	Encrypted IKE messages protected by this suite are encrypted using AES with a 128-bit key.
aes-192	Encrypted IKE messages protected by this suite are encrypted using AES with a 192-bit key.
aes-256	Encrypted IKE messages protected by this suite are encrypted using AES with a 256-bit key.
des	Specifies 56-bit DES-CBC as the encryption algorithm to be used in the IKE policy.
3des	Specifies that the 3DES encryption algorithm is to be used in the IKE policy.
group1	Specifies that the 768-bit DH group is to be used in the IKE policy. This is the default value.
group2	Specifies that the 1024-bit DH group 2 be used in the IKE policy.
group5	Specifies that the 768-bit DH group is to be used in the IKE policy. This is the default value.
group7	Specifies that IPSec should use group7 (Elliptic Curve Cryptography [ECC]) where the elliptical curve field size is 163 bits, for example, with the Movian VPN client.
Lifetime *seconds*	Specifies how many seconds each SA should exist before expiring. To propose a finite lifetime, use an integer from 120 to 86,400 seconds (one day). Specify 0 seconds for infinite lifetime.
md5	Specifies MD5 (Hash-based Message Authentication Code [HMAC] variant) as the hash algorithm to be used in the IKE policy.
pre-share	Specifies pre-shared keys as the authentication method.
priority	Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 65534, with 1 being the highest priority and 65534 the lowest.
rsa-sig	Specifies RSA Signature as the authentication method. RSA Signature provides nonrepudiation for the IKE negotiation. This basically means that you can prove to a third party whether you had an IKE negotiation with the peer.
dsa-sig	Specifies Directory System Agent (DSA) Signature as the authentication method.
sha	Specifies SHA-1 (HMAC variant) as the hash algorithm to be used in the IKE policy. This is the default hash algorithm.

Task 2: Create IP Address Pool

Cisco.com

Remote Client

172.26.26.1

Internet

Outside

192.168.1.5

Inside

Server
10.0.0.15

vpnpool
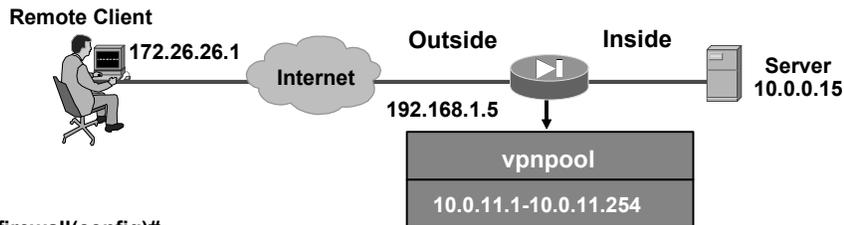
10.0.11.1-10.0.11.254

firewall(config)#

```
ip local pool poolname first-address—last-address [mask
  mask]
```

• **Creates an optional local address pool if the remote
  client is using the remote server as an external
  DHCP server**

```
fw1(config)# ip local pool MYPOOL 10.0.11.1-10.0.11.254
```

SNPA v4.0—12-31

If you are using a local IP address pool, you must also configure that pool. Use the **ip local pool** command. The syntax for this command is as follows:

```
ip local pool poolname first-address—last-address [mask mask]
```

first-address	Specifies the starting address in the range of IP addresses
last-address	Specifies the final address in the range of IP addresses
mask *mask*	(Optional) Specifies a subnet mask for the pool of addresses
poolname	Specifies the name of the IP address pool

Task 3: Define Group Policy for Mode Configuration Push

Task 3 contains the following steps:

- **Step 1: Set the tunnel group type.**
- **Step 2: Configure the IKE pre-shared key.**
- **Step 3: Specify the local IP address pool.**
- **Step 4: Configure the group policy type.**
- **Step 5: Enter the group-policy attributes submode.**
- **Step 6: Specify the DNS servers.**
- **Step 7: Specify the WINS servers.**
- **Step 8: Specify the DNS domain.**
- **Step 9: Specify idle timeout.**

Complete this task to define a group policy to be pushed during mode configuration. Although users can belong to only one group per connection, they may belong to specific groups with different policy requirements.

Beginning in global configuration mode, use the following steps to define the policy attributes that are pushed to the Cisco VPN Client via mode configuration:

Step 119 Set the tunnel group type

Step 120 Configure the IKE pre-shared key.

Step 121 Specify the local IP address pool.

Step 122 Configure the group policy type.

Step 123 Enter the group policy attributes submode.

Step 124 Specify the DNS servers.

Step 125 Specify the WINS servers.

Step 126 Specify the DNS domain.

Step 127 Specify the idle timeout.

Step 1: Set the Tunnel Group Type
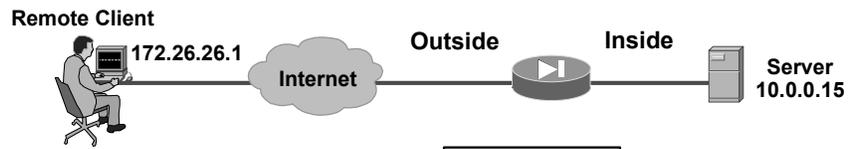
Remote Client
172.26.26.1

Internet

Outside   Inside

Server
10.0.0.15

Push
to Client

VPN Group
Pre-Share
DNS Server
WINS Server
DNS Domain
Address Pool
Idle Time

firewall(config)#

```
tunnel-group name type type
```

- **Names the tunnel group**
- **Defines the type of VPN connection that is to be established**

```
fw1(config)# tunnel-group training type ipsec-ra
```

SNPA v4.0—12-33

Step 128   To enable remote access, the tunnel group type must be named and set to remote access using the **ipsec-ra** command.

Step 2: Configure IKE Pre-Shared Key
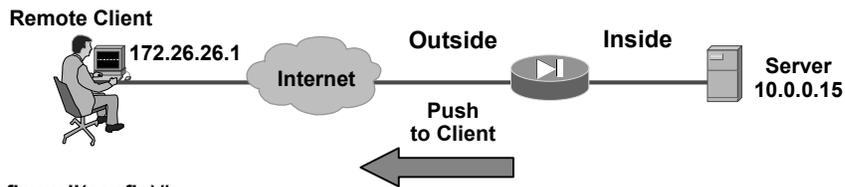
Remote Client
172.26.26.1

Internet

Outside   Inside

Push
to Client

Server
10.0.0.15

firewall(config)#

```
tunnel-group name [general-attributes | ipsec-attributes]
```

• **Enters tunnel-group ipsec-attributes submode to configure the key**

firewall(config-ipsec)#

```
pre-shared-key key
```

• **Associates a pre-shared key with the connection policy**

```
fw1(config)# tunnel-group training ipsec-attributes
fw1(config-ipsec)# pre-shared-key cisco123
```

SNPA v4.0—12-34

Step 129   Use the **pre-shared-key** command to specify the IKE pre-shared key when defining group policy information for the mode configuration push. You must use this command if the Cisco VPN Client identifies itself to the router with a pre-shared key.

The syntax for the **pre-shared-key** command is as follows:

```
pre-shared-key key
```

key	Specifies an alphanumeric key between one and 128 characters.

Step 3: Specify Local IP Address Pool
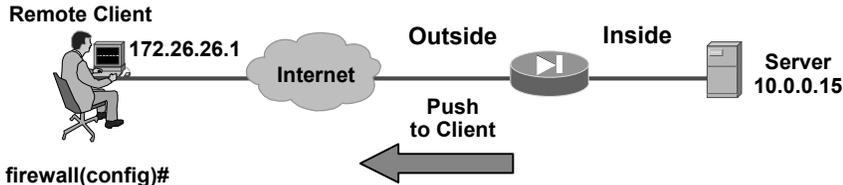
Remote Client
172.26.26.1

Internet

Outside   **Inside**

Server
10.0.0.15

**Push
to Client**

firewall(config)#

```
tunnel-group name [general-attributes | ipsec-attributes]
```

• **Enters tunnel-group general-attributes submode to configure the address pool**

firewall(config-general)#

```
address-pool [interface name] address_pool1
  [...address_pool6]
```

• **Associates an address pool with the connection policy**

```
fw1(config)# tunnel-group training general-attributes
fw1(config-general)# address-pool MYPOOL
```

Step 130   Use the **address-pool** command to refer to an IP local pool address, which defines a range of addresses that will be used to allocate an internal IP address to a VPN client.

Use the **address-pool** command in the general-attributes subcommand mode to define a local pool address.

The syntax for the **address-pool** command is as follows:

```
address-pool [interface name] address_pool1 [...address_pool6]
```

address_pool	Specifies the name of the address pool configured with the **ip local pool** command. You can specify up to six local address pools.
interface name	(Optional) Specifies the interface to be used for the address pool.

Step 4: Configure the Group Policy Type

Cisco.com
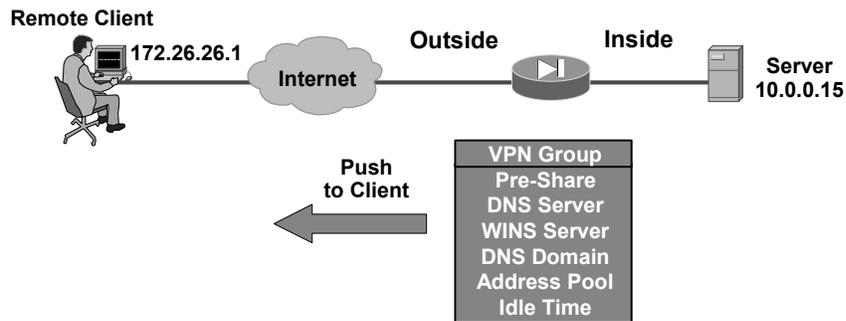
Remote Client
172.26.26.1

Internet

Outside   Inside

Server
10.0.0.15

Push
to Client

VPN Group
Pre-Share
DNS Server
WINS Server
DNS Domain
Address Pool
Idle Time

firewall(config)#

```
group-policy {name internal [from group-policy name]}
```

```
fw1(config)# group-policy training internal
```

SNPA v4.0—12-36

Step 131   Use the **group-policy** command to create and specify the type of group to be created.

Step 5: Enter the Group-Policy Attributes Subcommand Mode
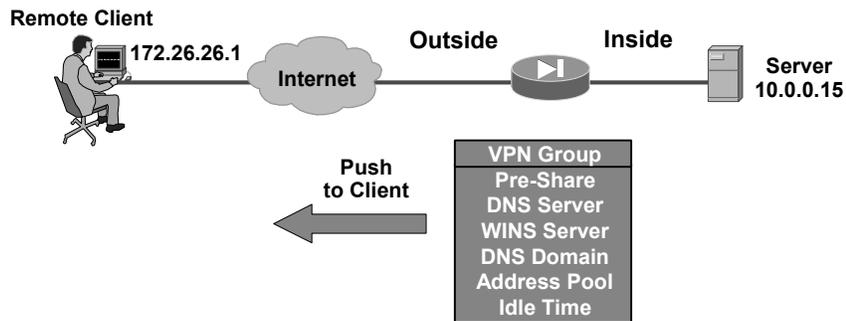
Remote Client
172.26.26.1

Internet

Outside   Inside

Server
10.0.0.15

Push
to Client

VPN Group
Pre-Share
DNS Server
WINS Server
DNS Domain
Address Pool
Idle Time

firewall(config)#

```
group-policy {name} attributes
```

```
fw1(config)# group-policy training attributes
fw1(config-group-policy)#
```

SNPA v4.0—12-37

Step 132   Enter the group-policy attribute subcommand mode to configure parameters specific to the group you created.

Step 6: Specify DNS Servers

Remote Client

172.26.26.1

Internet

Outside   **Inside**

Server
10.0.0.15

Push to Client

VPN Group
Pre-Share
DNS Server
WINS Server
DNS Domain
Address Pool
Idle Time
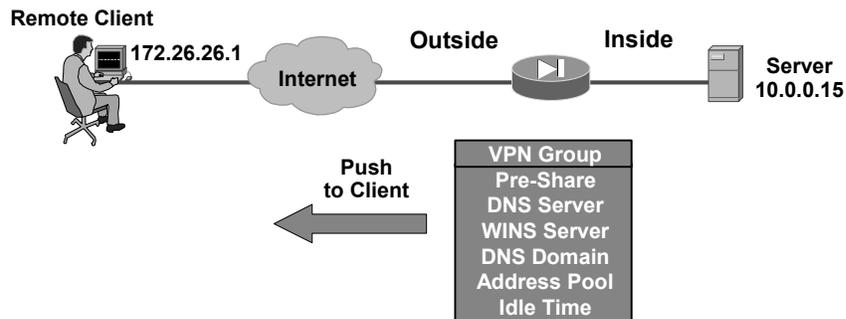
firewall(config-group-policy)#

```
dns-server {value ip_address [ip_address] | none}
```

```
fw1(config-group-policy)# dns-server value 10.0.0.15
```

SNPA v4.0—12-38

Step 133 (Optional) Specify the primary and secondary DNS servers using the **dns-server** command in group-policy configuration mode.

Every time you issue the **dns-server** command, you overwrite the existing setting. For example, if you configure DNS server x.x.x.x, then configure DNS server y.y.y.y, the second command overwrites the first and y.y.y.y becomes the sole DNS server. The same holds true for multiple servers. To add a DNS server rather than overwrite previously configured servers, include the IP addresses of all DNS servers when you enter this command.

The syntax for the **dns-server** command is as follows:

```
dns-server {value ip_address [ip_address] | none}
```

none	Sets WINS servers to a null value, thereby allowing no DNS servers. Prevents inheriting a value from a default or specified group policy.
value *ip_address*	Specifies the IP address of the primary and secondary DNS servers.

Step 7: Specify WINS Servers

Step 134 (Optional) Specify the primary and secondary WINS servers using the **wins-server** command in group-policy configuration mode.

As with DNS servers, every time you issue the **wins-server** command, you overwrite the existing setting.

The syntax for the **wins-server** command is as follows:

```
wins-server value {ip_address} [ip_address] | none
```

none	Sets WINS servers to a null value, thereby allowing no WINS servers. Prevents inheriting a value from a default or specified group policy.
value *ip_address*	Specifies the IP address of the primary and secondary WINS servers.

Step 8: Specify DNS Domain

Remote Client 172.26.26.1

Outside **Inside**

Internet

Server 10.0.0.15 Cisco.com

Push to Client

VPN Group
Pre-Share
DNS Server
WINS Server
DNS Domain
Address Pool
Idle Time
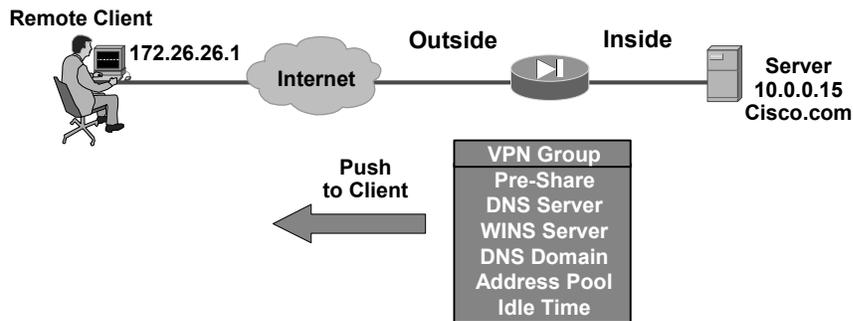
firewall(config-group-policy)#

```
default-domain {value domain-name | none}
```

```
fw1(config-group-policy)# default-domain value cisco.com
```

SNPA v4.0—12-40

Step 135 (Optional) Specify the DNS domain to which a group belongs by using the **default-domain** command in group-policy configuration mode.

The security appliance passes the default domain name to the IPSec client to append to DNS queries that omit the domain field. This domain name applies only to tunneled packets. When there are no default domain names, users inherit the default domain name in the default group policy.

The syntax for the **default-domain** command is as follows:

```
default-domain {value domain-name | none}
```

none	Indicates that there is no default domain name. Sets a default domain name with a null value, thereby disallowing a default domain name. Prevents inheriting a default domain name from a default or specified group policy.
value *domain-name*	Identifies the default domain name for the group.

Step 9: Specify Idle Timeout
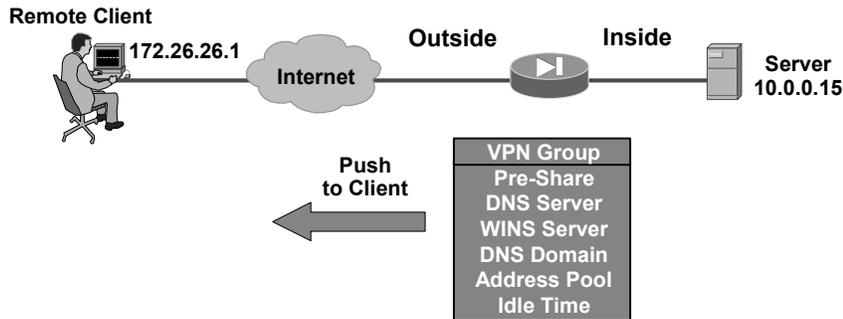
Remote Client
172.26.26.1

Outside   **Inside**

Internet

Server
10.0.0.15

**Push
to Client**

VPN Group
Pre-Share
DNS Server
WINS Server
DNS Domain
Address Pool
Idle Time

firewall(config-group-policy)#

```
vpn-idle-timeout {minutes | none}
```

```
fw1(config-group-policy)# vpn-idle-timeout 600
```

SNPA v4.0—12-41

Step 136 (Optional) Use the **vpn-idle-timeout** command to set the inactivity timeout for a Cisco VPN Client. When the inactivity timeout for a given VPN client or Easy VPN Remote device expires, the tunnel is terminated. The default inactivity timeout is 30 minutes.

The syntax for the **vpn-idle-timeout** command is as follows:

```
vpn-idle-timeout {minutes | none}
```

minutes	Specifies the number of minutes in the timeout period. Use an integer between 1 and 35791394.
none	Permits an unlimited idle timeout period. Sets idle timeout with a null value, thereby disallowing an idle timeout. Prevents inheriting a value from a default or specified group policy.

Task 4: Create Transform Set

Cisco.com

Remote Client
172.26.26.1

Internet

Outside **Inside**

Server 10.0.0.15

192.168.1.5

Transform Set
DES
SHA-HMAC
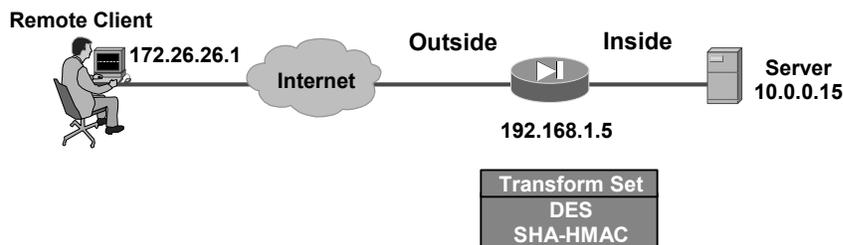
firewall(config)#

```
crypto ipsec transform-set transform-set-name transform1
  [transform2]]
```

```
fw1(config)# crypto ipsec transform-set remoteuser1
  esp-des esp-sha-hmac
```

SNPA v4.0—12-42

Use the **crypto ipsec transform-set** command to specify which transform sets are allowed for the crypto map entry. When using this command, be sure to list multiple transform sets in order of priority (highest priority first). Note that this is the only configuration statement that is required in dynamic crypto map entries.

The syntax for the **crypto ipsec transform-set** command is as follows:

```
crypto ipsec transform-set transform-set-name transform1
[transform2]
```

transform-set-name	Specifies the name of the transform set to create or modify.
transform1, transform2	Specifies up to two transforms. Transforms define the IPSec security protocol(s) and algorithm(s). Each transform represents an IPSec security protocol (ESP), plus the algorithm to use, either [**esp-aes** | **esp-aes-192** | **esp-aes-256** | **esp-des** | **esp-3des** | **esp-null** | **esp-none**] or [**esp-md5-hmac** | **esp-sha-hmac**].

Task 5: Create Dynamic Crypto Map

Remote Client

172.26.26.1

Internet

Outside

Inside

Server
10.0.0.15

192.168.1.5
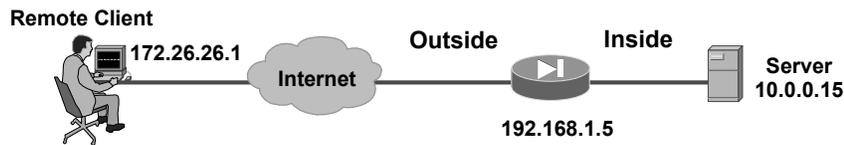
firewall(config)#

```
crypto dynamic-map dynamic-map-name dynamic-seq-num set
  transform-set transform-set-name1 [… transform-set-
  name9]
```

```
fw1(config)# crypto dynamic-map rmt-dyna-map 10 set
  transform-set remoteuser1
```

SNPA v4.0—12-43

Use the **crypto dynamic-map** command to create a dynamic crypto map entry and enter the crypto map configuration mode.

The syntax for the **crypto dynamic-map** command is as follows:

```
crypto dynamic-map dynamic-map-name dynamic-seq-num set
transform-set transform-set-name1 [… transform-set-name9]
```

dynamic-map-name	Specifies the name of the dynamic crypto map set.
dynamic-seq-num	Specifies the number of the dynamic crypto map entry.
transform-set-name1 *transform-set-name9*	Identifies the transform set to be used with the dynamic crypto map entry (the names of transform sets that have been defined using the **crypto ipsec** command).

A dynamic crypto map entry is essentially a crypto map entry without all the parameters configured. It acts as a policy template in which the missing parameters are later dynamically configured (as the result of an IPSec negotiation) to match a remote peer's requirements. This allows remote peers to exchange IPSec traffic with the router even if the router does not have a crypto map entry specifically configured to meet all of the remote peer's requirements.

Dynamic crypto maps are not used by the router to initiate new IPSec SAs with remote peers. Dynamic crypto maps are used when a remote peer tries to initiate an IPSec SA with the router. Dynamic crypto maps are also used in evaluating traffic.

Task 6: Assign Dynamic Crypto Map to Static Crypto Map

Remote Client
172.26.26.1

Internet

Outside

Inside

Server
10.0.0.15

192.168.1.5
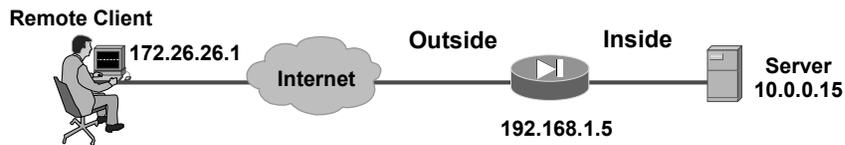
firewall(config)#

```
crypto map map-name seq-num ipsec-isakmp dynamic dynamic-
  map-name
```

```
fw1(config)# crypto map rmt-user-map 10 ipsec-isakmp
  dynamic rmt-dyna-map
```

SNPA v4.0—12-44

Add the dynamic crypto map to a static crypto map. The syntax for the command is as follows:

```
crypto map map-name seq-num ipsec-isakmp dynamic dynamic-map-
name
```

dynamic-map-name	Specifies the name of the crypto map entry that refers to a preexisting dynamic crypto map
ipsec-isakmp	Indicates that IKE establishes the IPSec SAs for this crypto map entry
map-name	Specifies the name of the crypto map set
seq-num	Specifies the number you assign to the crypto map entry

Task 7: Apply Dynamic Crypto Map to Security Appliance Outside Interface

Remote Client

172.26.26.1

Internet

Outside   **Inside**

Server 10.0.0.15

192.168.1.5
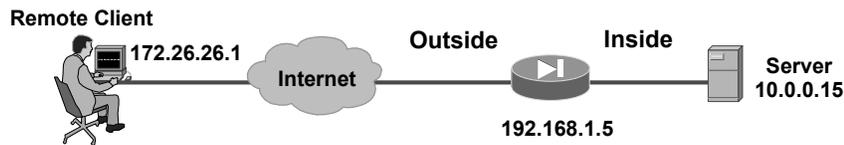
firewall(config)#

```
crypto map map-name interface interface-name
```

```
fw1(config)# crypto map rmt-user-map interface
  outside
```

SNPA v4.0—12-45

Apply the crypto map to the security appliance outside interface. The syntax for the command is as follows:

```
crypto map map-name interface interface-name
```

map-name	Specifies the name of the crypto map set.
interface-name	Specifies the interface for the security appliance to use for establishing tunnels with VPN peers. If ISAKMP is enabled, and you are using a CA to obtain certificates, this should be the interface with the address specified in the CA certificates.

Complete the following steps to configure Xauth on your Easy VPN Server router:

Step 137 Enable AAA login authentication.

Step 138 Define AAA server IP address and encryption key.

Step 139 Enable IKE Xauth for the crypto map.

Step 1: Enable AAA Login Authentication

Remote Client
172.26.26.1

Internet

Outside   **Inside**

**TACACS+
Server
10.0.0.15**

192.168.1.5
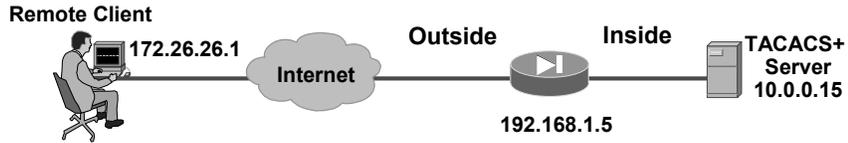
firewall(config)#

```
aaa-server server-tag protocol server-protocol
```

```
fw1(config)# aaa-server mytacacs protocol tacacs+
fw1(config-aaa-server-group)#
```

Step 140   Enable AAA login authentication using the **aaa server protocol** command.

The syntax for the **aaa server protocol** command is as follows:

```
aaa-server server-tag protocol server-protocol
```

server-tag	Symbolic name of the server group. Other **aaa** commands make reference to the *server-tag* group as defined by the **aaa-server** command *server-tag* parameter.
server-protocol	The AAA protocol that the servers in the group support: **kerberos**, **ldap**, **nt**, **radius**, **sdi**, or **tacacs+**.

Step 2: Define AAA Server IP Address and Encryption Key

Remote Client
172.26.26.1

Outside   **Inside**   **TACACS+ Server** 10.0.0.15

Internet

192.168.1.5
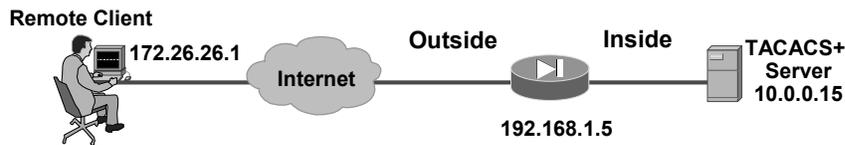
firewall(config)#

```
aaa-server server-tag [(interface-name)] host server-ip
  [key] [timeout seconds]
```

```
fw1(config)# aaa-server mytacacs (inside) host 10.0.0.15
  cisco123 timeout 5

fw1(config-aaa-server-host)#
```

Step 141   Set the IP address of the AAA server and the encryption key using the **aaa-server host** command.

The syntax for the **aaa-server host** command is as follows:

```
aaa-server server-tag [(interface-name)] host server-ip [key]
[timeout seconds]
```

interface-name	(Optional) The network interface where the authentication server resides. The parentheses are required in this parameter.
key	(Optional) A case-sensitive, alphanumeric keyword of up to 127 characters that is the same value as the key on the RADIUS or TACACS+ server. Any characters entered past 127 are ignored. The key is used between the security appliance and the server for encrypting data between them. The key must be the same on both the security appliance and the server systems. Spaces are not permitted in the key, but other special characters are allowed. You can add or modify the key using the **key** command in host mode.
server-ip	The IP address of the AAA server.
server-tag	Symbolic name of the server group. Other **aaa** commands make reference to the *server-tag* group as defined by the **aaa-server** command *server-tag* parameter.
timeout *seconds*	(Optional) The timeout interval for the request. This is the time after which the security appliance gives up on the request to the primary AAA server. If there is a standby AAA server, the security appliance sends the request to the backup server. You can modify the timeout interval using the **timeout** command in host mode.

Step 142 Enable IKE Xauth for the tunnel using the **authentication-server-group** command in tunnel-group general-attributes configuration mode**.**

The syntax for the **authentication-server-group** command is as follows:
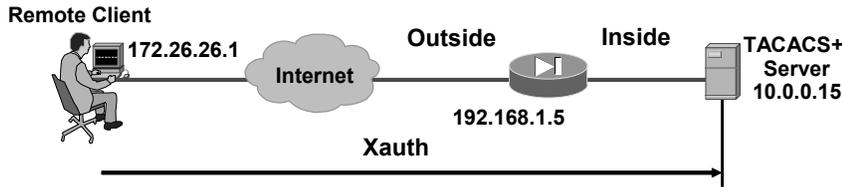
```
authentication-server-group [(interface name)] server group
[LOCAL | NONE]
```

interface name	(Optional) Specifies the interface that the authentication server is on.
LOCAL	(Optional) Specifies authentication that is to be performed against the local user database if all of the servers in the server group have been deactivated because of communication failures. If the server group name is either LOCAL or NONE, do not use the **LOCAL** keyword here.
NONE	(Optional) Specifies the server group name as NONE. To indicate that authentication is not required, use the **NONE** keyword as the server group name.
server group	Specifies the name of the AAA server group, which defaults to LOCAL.

Task 9: Configure NAT and NAT 0

Cisco.com

Remote Client

10.0.11.0

Internet

Outside

Inside
10.0.0.0

TACACS+ Server
10.0.0.15

192.168.1.5

Encrypted — No Translation

Clear Text — Translation
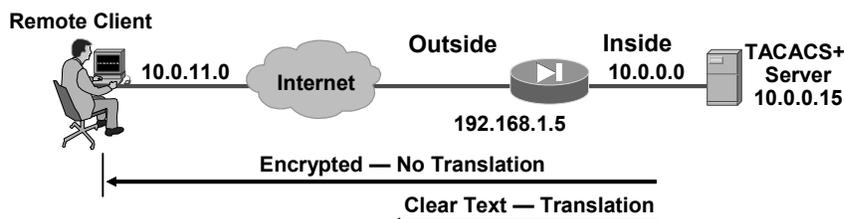
```
fw1(config)# access-list 101 permit ip 10.0.0.0
  255.255.255.0 10.0.11.0 255.255.255.0
fw1(config)# nat (inside) 0 access-list 101
fw1(config)# nat (inside) 1 0.0.0.0 0.0.0.0 0 0
fw1(config)# global (outside) 1 interface
```

- **Matches ACL: Encrypted data and no translation (NAT 0)**
- **Does not match ACL: Clear text and translation (PAT)**

SNPA v4.0—12-50

The last task is to define which traffic is encrypted and sent down the IPSec tunnel and which traffic is translated and transmitted in clear text. The **nat 0 access-list** command defines which traffic is encrypted but not translated. In the figure, traffic that is sourced from network 10.0.0.0/24 and destined for a host on network 10.0.11.0/24 is encrypted. The remaining traffic is translated, using NAT, to the IP address of the outside interface, then transmitted in clear text.

The syntax for the **nat 0 access-list** command is as follows:

```
nat (real_ifc) 0 access-list access_list_name
```

access-list	Associates **access-list** command statements with the **nat 0** command and exempts traffic that matches the ACL from NAT processing.
access_list_name	The ACL name.
real_ifc	The name of the network interface, as specified by the **nameif** command, through which the hosts or network designated by local_ip are accessed.

Task 10: Enable IKE DPD

Cisco.com

Remote Client

10.0.11.0   Internet   **Outside**   **Inside**   10.0.0.0   **TACACS+ Server** 10.0.0.15

1) DPD Send: Are you there?

2) DPD Reply: Yes, I am here.
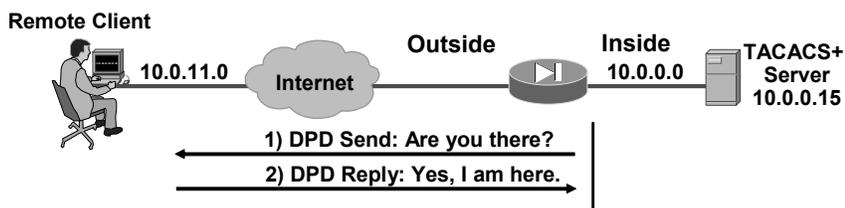
`firewall(config-ipsec)#`

```
isakmp keepalive [threshold seconds] [retry seconds]
  [disable]
```

• **Configures the IKE DPD parameters**

```
fw1(config)# tunnel-group training ipsec-attributes
fw1(config-ipsec)# isakmp keepalive threshold 30 retry 10
```

SNPA v4.0—12-51

DPD allows two IPSec peers to determine if the other is still "alive" during the lifetime of a VPN connection. DPD is useful because a host may reboot or the dialup link of a remote user may disconnect without notifying the peer that the VPN connection has gone away. When the IPSec host determines that a VPN connection no longer exists, it can notify the user, attempt to switch to another IPSec host, or clean up valuable resources that were allocated for the peer that no longer exists.

A DPD peer can send DPD messages, reply to DPD messages, or both. DPD messages are unidirectional and are automatically sent by Cisco VPN Clients. Unlike the old-style IKE keepalives, DPD is not required on both peers. You can configure DPD on only the remote, only the headend, or both, depending on the requirements. Use the **isakmp keepalive** command in tunnel-group ipsec-attributes configuration mode to enable a security appliance gateway to send IKE DPD messages. You can specify the number of seconds between DPD messages, for example, 30 seconds. You can also specify the number of seconds between retries if a DPD message fails, for example, 10 seconds.

The syntax of the command is as follows:

```
isakmp keepalive [threshold seconds] [retry seconds] [disable]
```

disable	Disables IKE keepalive processing, which is enabled by default.
retry *seconds*	Specifies the interval in seconds between retries after a keepalive response has not been received. The range is 2 to 10 seconds. The default is 2 seconds.
threshold *seconds*	Specifies the number of seconds the peer can idle before beginning keepalive monitoring. The range is 10 to 3600 seconds. The default is 10 seconds.

Easy VPN Server Configuration Summary

```
PIX Version 7.0(1)
hostname fw1
!--- Configure Phase 1 Internet Security Association
!-- and Key Management Protocol (ISAKMP) parameters.
isakmp enable outside
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption aes
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400

!--- Configure IPSec transform set and dynamic crypto map.
crypto ipsec transform-set myset esp-aes esp-md5-hmac
crypto dynamic-map rmt-dyna-map 10 set transform-set myset
crypto map rmt-user-map 10 ipsec-isakmp dynamic rmt-dyna-map
!--- Apply crypto map to the outside interface.
crypto map rmt-user-map interface outside
```

SNPA v4.0—12-52

The next few examples display the security appliance Easy VPN Server configuration. The example in the figure here highlights the *isakmp* and *crypto map* parameters of the configuration.

Easy VPN Server Configuration Summary (Cont.)

```
!--- Configure remote client pool of IP addresses
ip local pool ippool 10.0.11.1-10.0.11.254
!--- Configure group policy parameters.
group-policy training internal
group-policy training attributes
 wins-server value 10.0.0.15
  dns-server value 10.0.0.15
 vpn-idle-timeout 600
 default-domain value cisco.com
 !--- Configure tunnel group policy parameters.
tunnel-group training type ipsec-ra
tunnel-group training general-attributes
 address-pool ippool
 authentication-server-group MYTACACS
 defaultgroup-policy training
tunnel-group training ipsec-attributes
 pre-shared-key training
 isakmp keepalive threshold 30 retry 10
```

SNPA v4.0—12-53

This figure highlights the address pool, group policy, and tunnel group parameters of the configuration. The security appliance will also send DPD messages to the Cisco VPN Client every 30 seconds. If the client fails to respond, the security appliance will resend the message after waiting 10 seconds.

Easy VPN Server Configuration Summary (Cont.)

```
!--- Configure AAA-Server parameters.
aaa-server MYTACACS protocol tacacs+
aaa-server MYTACACS host 10.0.0.15
 timeout 5
 key secretkey
!--- Specify "nonat" access list.
access-list 101 permit ip 10.0.0.0 255.255.255.0 10.0.11.0
  255.255.255.0
!--- Configure Network Address Translation (NAT)/
!--- Port Address Translation (PAT) for regular traffic,
!--- as well as NAT for IPSec traffic.
nat (inside) 0 access-list 101
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
global (outside) 1 interface
```

This figure highlights the authentication, NAT 0, NAT, and global parameters of the configuration. Any traffic between 10.0.0.0/24 and 10.0.11.0/24 will not be translated by the security appliance. Any other traffic will be translated using the outside interface address of the security appliance.

Configure Security Appliance Hub-and-Spoke VPNs

This topic contains information regarding the configuration of hub-and-spoke VPNs on the security appliance.

Benefits of Hub-and-Spoke VPNs

Telecommuter—Spoke

Remote Site—Spoke

Central site

Server—Spoke

Internet

Hub

Mobile—Spoke

- Provide support for small sites with small LAN and low-end PIXs because only one IPSec tunnel is needed at the spoke routers.
- Scale the network through scaling of the network at specific hub point.
- Only the hub needs to have a static and global IP address. All the spoke PIXs can have DHCP-based dynamic IP address, with the hub configured with dynamic crypto map.
- Very easy to add sites and security appliances, as no changes to the existing spoke or hub security appliance are required.

SNPA v4.0—12-56

In hub-and-spoke network configurations, the spoke sites connect via IPSec tunnels to a hub site to establish connectivity to the network. The hub site consists of high-end tunnel aggregation routers servicing multiple IPSec tunnels for a predefined maximum number of spoke locations.

In addition, by terminating the VPN tunnels at the hub site, the headend can act as the distribution point for all routing information and connectivity to and from spoke site devices. For resiliency and load distribution, the hub site can be made with multiple headend devices.

Limitations of Benefits of Hub-and-Spoke VPNs

Telecommuter—Spoke

Remote Site—Spoke

Central site

Server—Spoke

Internet

Hub

Mobile—Spoke
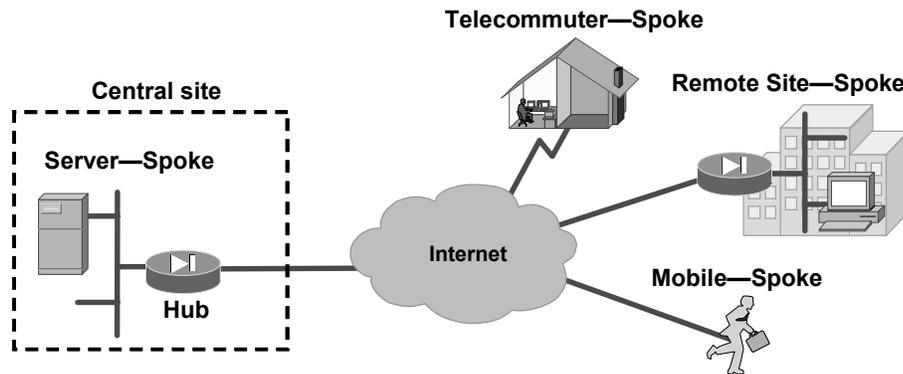
- **IPSec performance is aggregated at the hub.**
- **All spoke-spoke packets are decrypted and reencrypted at the hub.**
- **When using hub-and-spoke with dynamic crypto maps, the IPSec encryption tunnel must be initiated by the spoke routers.**

SNPA v4.0—12-57

The hub-and-spoke design is the most suitable configuration when the majority of traffic is targeted to the hub and the core of the network. Some spoke sites may require direct access. Additional IPSec connections that form partial mesh connections can enable a direct IPSec path.

Configure Hub-and-Spoke VPN

- **VPN spokes can be terminated on a single interface.**
- **Traffic from the same security level can also be permitted.**

Telecommuter—Spoke

Remote Site—Spoke

Server—Spoke

30.0.0.0

40.0.0.0

Internet

Mobile—Spoke

10.0.0.0

Hub

50.0.0.0
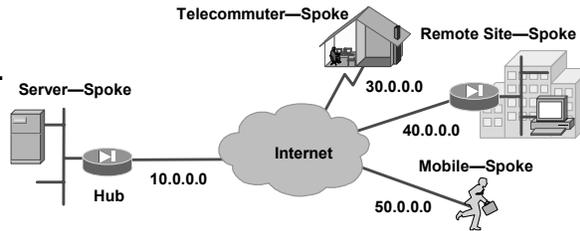
firewall(config)#

```
same-security-traffic permit [inter-interface | intra-
  interface]
```

- **Permits communication between different interfaces with the same security level or between VPN peers connected to the same interface**

```
fw1(config)# same-security-traffic permit intra-interface
```

SNPA v4.0—12-58

All of the VPN spokes can be terminated on a single interface by using the **same-security-traffic** command. This command also permits traffic between interfaces that have the same security levels.

The syntax of the command is as follows:

```
same-security-traffic permit {inter-interface | intra-
interface}
```

inter-interface	Permits communication between different interfaces that have the same security level
intra-interface	Permits communication in and out of the same interface when traffic is IPSec-protected

Cisco VPN Client Manual Configuration Tasks

This topic contains information regarding the installation and configuration of the Cisco VPN Client.

Cisco VPN Client Manual Configuration Tasks

The following general tasks are used to configure Cisco VPN Client:

- **Task 1: Install Cisco VPN Client.**
- **Task 2: Create a new connection entry.**
- **Task 3: (Optional) Configure Cisco VPN Client transport properties.**
- **Task 4: (Optional) Configure Cisco VPN Client backup servers properties.**
- **Task 5: (Optional) Configure Dialup properties.**

SNPA v4.0—12-60

Use the following steps to install and configure the Cisco VPN Client:

Step 143   Install Cisco VPN Client.

Step 144   Create a new connection entry.

Step 145   (Optional) Configure Cisco VPN Client transport properties.

Step 146   (Optional) Configure properties of Cisco VPN Client backup servers.

Step 147   (Optional) Configure dialup properties.

Task 1: Install Cisco VPN Client
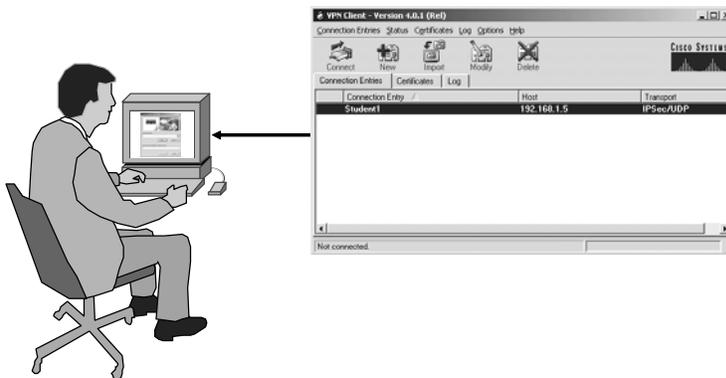
SNPA v4.0—12-61

Installation of the Cisco VPN Client varies slightly based on the type of operating system. Always review the installation instructions that come with the Cisco VPN Client before attempting any installation. Generally, installation of the VPN Client involves the following steps (this example is based on installing the VPN Client on a Windows 2000 PC):

Step 148 Open the Cisco VPN Client folder that is on the student PC desktop.

Step 149 Double-click the setup.exe file that is in the Cisco VPN Client folder. If this is the first time that the Cisco VPN Client is being installed on this PC, a window opens and displays the following message: "Do you want the installer to disable the IPSec Policy Agent?"

Step 150 If the disable IPSec policy agent message appears, click **Yes**. The Welcome window opens.

Step 151 Read the Welcome window and click **Next**. The License Agreement window opens.

Step 152 Read the license agreement and click **Yes**. The Destination Folder Location window opens.

Step 153 Accept the defaults by clicking **Next**. The Program Folders window opens.

Step 154 Accept the defaults by clicking **Next**. The Start Copying Files window opens.

Step 155 The files are copied to the hard disk drive of the student PC, and the InstallShield Wizard Complete window opens.

Step 156 Select **Yes, I want to restart my computer now** and click **Finish**. The PC restarts.

This completes the installation of the Cisco VPN Client.

Task 2: Create New Connection Entry

SNPA v4.0—12-62

The Cisco VPN Client enables users to configure multiple connection entries. Multiple connection entries enable the user to build a list of possible network connection points. For example, a corporate telecommuter may want to connect to the sales office in Boston for sales data (the first connection entry), then the telecommuter and the sales office may want to connect to the Austin factory for inventory data (a second connection entry). Each connection contains a specific entry name and remote server hostname or IP address.

The Easy VPN Server and the Cisco VPN Client connection can be authenticated either with the group name and password or with digital certificates. The Authentication tab enables you to set your authentication information. You need to choose one method, group, or certificate via the radio buttons.

Within the Group Authentication information group box in the Authentication tab, enter the group name and password in the appropriate fields. The group name and password must match what is configured for this group within the Easy VPN Server. Entries are case sensitive.

For certificates to be exchanged, the Certificate Authentication radio button must be selected. In the Name drop-down menu, any personal certificates that are loaded on your PC are listed. Choose the certificate to be exchanged with the Easy VPN Server during connection establishment. If no personal certificates are loaded in your PC, the drop-down menu is blank.

Generally, creating a new connection entry involves the following steps (this example is based on creating new connection entries on a Windows 2000 PC):

Step 157   Choose **Start > Programs > Cisco Systems VPN Client > VPN Client**. The Cisco Systems VPN Client window opens.

Step 158   Click **New**. The New Connection Entry wizard opens.

Step 159   Enter a name for the new connection entry in the Name of the New Connection Entry field (for example, Boston Sales).

Step 160   Enter the public interface IP address or hostname of the remote Easy VPN Server in the Host field.

Step 161   Select **Group Authentication** and complete the following substeps. The following entries are always case sensitive:

7.   Enter a group name that matches a group on the Easy VPN Server.

8.   Enter the group password.

9.   Confirm the password.

Step 162   Click **Save**.

You have successfully configured the network parameters for the Cisco VPN Client and created a new VPN connection entry.
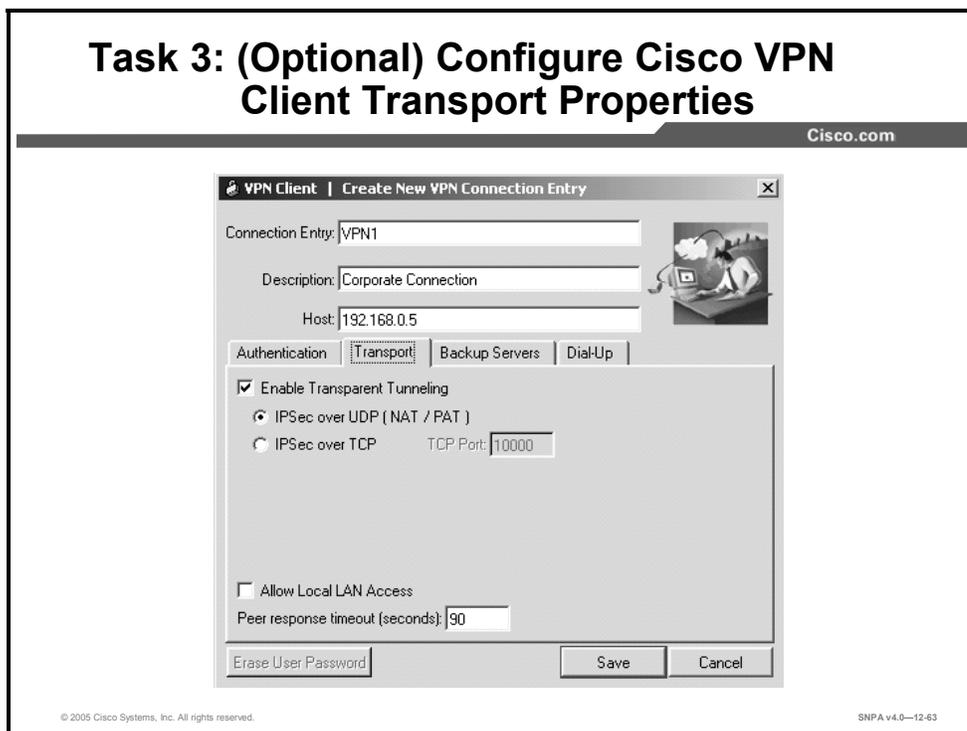
Transparent Tunneling

Transparent tunneling allows secure transmission between the Cisco VPN Client and a secure gateway through a router serving as a firewall, which may also be performing NAT or PAT. Transparent tunneling encapsulates Protocol 50 (ESP) traffic within UDP packets and can allow for both IKE (UDP 500) and Protocol 50 traffic to be encapsulated in TCP packets before it is sent through the NAT or PAT devices or firewalls. The most common application for transparent tunneling is behind a home router performing PAT. The central-site group in the Cisco VPN device must be configured to support transparent tunneling. This parameter is enabled by default. To disable this parameter, deselect the **Enable Transparent Tunneling** check box under the Transport tab. It is recommended that you always keep this parameter selected.

Note	Not all devices support multiple simultaneous connections behind them. Some cannot map additional sessions to unique source ports. Be sure to check with the vendor of your device to verify whether this limitation exists. Some vendors support Protocol 50 (ESP) PAT (IPSec pass-through), which might let you operate without enabling transparent tunneling.

You must choose a mode of transparent tunneling, over UDP or over TCP. The mode you use must match that used by the secure gateway to which you are connecting. Either mode operates properly through a PAT device. Multiple simultaneous connections might work better with TCP. If you are in an extranet environment, then in general, TCP mode is preferable. UDP does not operate with stateful firewalls, so in that case, you should use TCP.

The following transport tunneling options are available:

- **IPSec over UDP (NAT/PAT)**—Select this radio button to enable IPSec over UDP (NAT/PAT) . With UDP, the port number is negotiated. UDP is the default mode.

- **IPSec over TCP (NAT/PAT/Firewall)**—Select this radio button to enable IPSec over TCP. When using TCP, you must also enter the port number for TCP in the TCP port field. This port number must match the port number configured on the secure gateway. The default port number is 10000.

Allowing Local LAN Access

In a multiple-network-interface-card configuration, local LAN access pertains only to network traffic on the interface on which the tunnel was established. **Allow Local LAN Access** gives you access to the resources on your local LAN (printer, fax, shared files, and other systems) when you are connected through a secure gateway to a central-site VPN device. When this parameter is enabled and your central site is configured to permit it, you can access local resources while connected. When this parameter is disabled, all traffic from your Cisco VPN Client system goes through the IPSec connection to the secure gateway.

To enable this feature, select the **Allow Local LAN Access** check box; to disable it, deselect the check box. If the local LAN you are using is not secure, you should disable this feature. For example, you would disable this feature when you are using a local LAN in a hotel or airport.

A network administrator at the central site configures a list of networks at the VPN Client side that you can access. You can access up to ten networks when this feature is enabled. When local LAN access is allowed and you are connected to a central site, all traffic from your system goes through the IPSec tunnel except traffic to the networks excluded from doing so (in the network list).

When this feature is enabled and configured on the Cisco VPN Client and permitted on the central-site VPN device, you can see a list of the local LANs available by looking at the Routes table.

Adjusting the Peer Response Timeout Value

The Cisco VPN Client uses a keepalive mechanism, DPD, to check the availability of the VPN device on the other side of an IPSec tunnel. If the network is unusually busy or unreliable, you might need to increase the number of seconds to wait before the Cisco VPN Client decides that the peer is no longer active. The default number of seconds to wait before terminating a connection is 90 seconds. The minimum number you can configure is 30 seconds, and the maximum is 480 seconds.

- To adjust the setting, enter the number of seconds in the **Peer response timeout (seconds)** field. The Cisco VPN Client continues to send DPD requests every 5 seconds until it reaches the number of seconds specified by the peer response timeout value.

Task 4: (Optional) Configure Cisco VPN Client Backup Servers Properties

SNPA v4.0—12-64
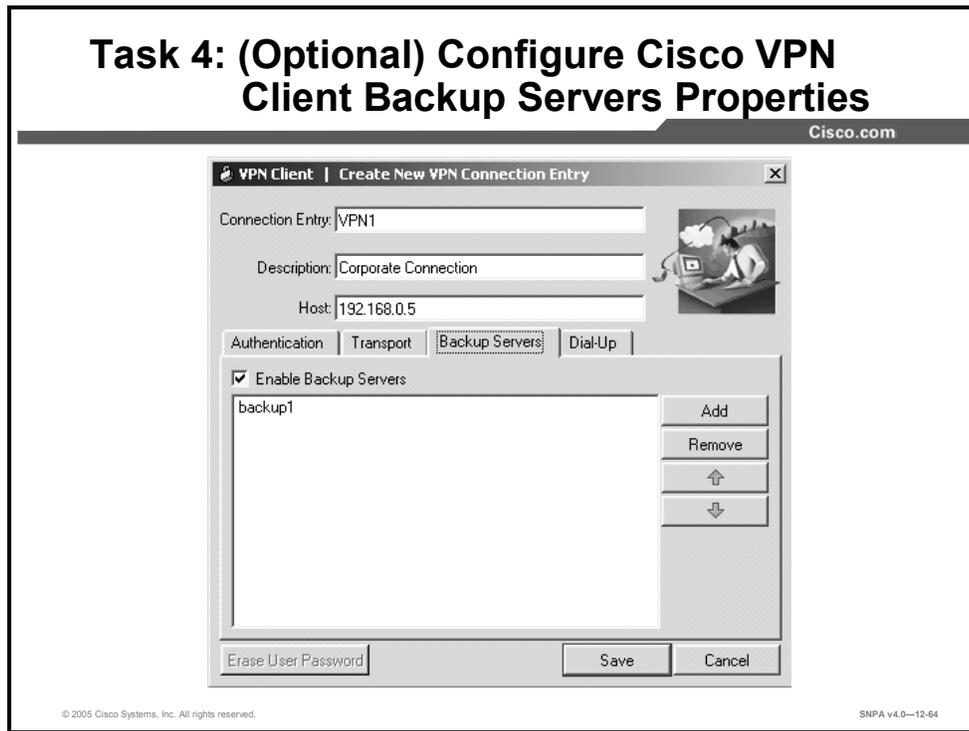
The private network may include one or more backup VPN servers to use if the primary server is not available. Your system administrator tells you whether to enable backup servers. Information on backup servers can download automatically from the Concentrator, or you can manually enter this information.

Task 5: (Optional) Configure Dialup Properties

SNPA v4.0—12-65
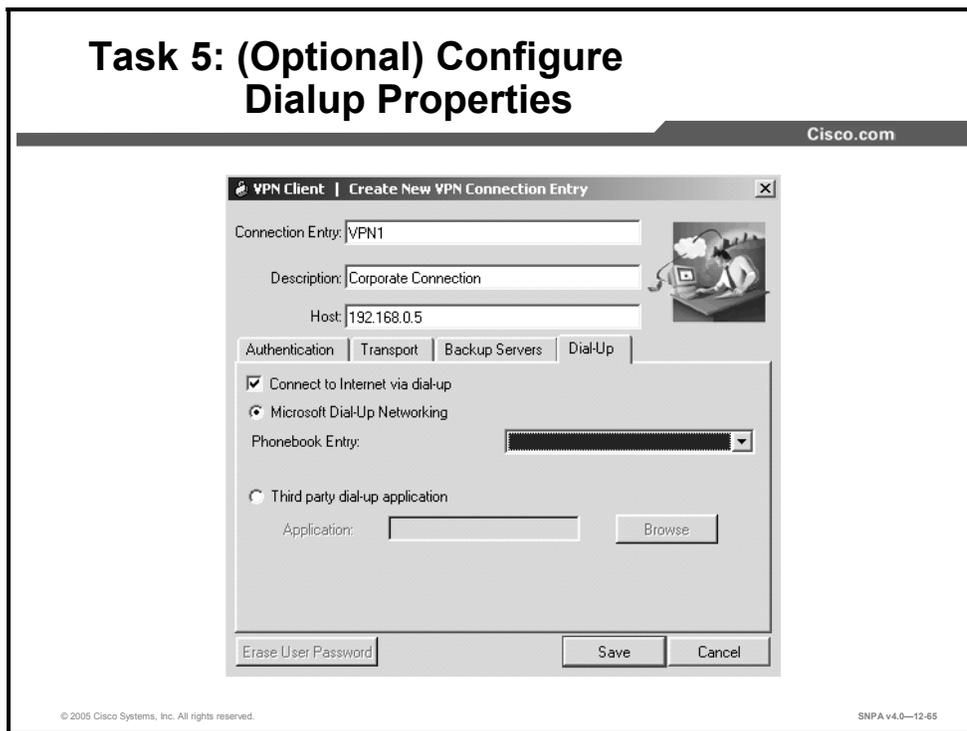
To enable and configure a connection to the Internet through dialup networking, select the **Connect to Internet via dial-up** check box. This feature is not selected by default.

You can connect to the Internet using the Cisco VPN Client application in either of the following ways:

■ Microsoft Dial-Up Networking (DUN)—If you have DUN phonebook entries and have enabled the Connect to Internet via dial-up feature, Microsoft DUN is enabled by default. To link your Cisco VPN Client connection entry to a DUN entry, click the **Phonebook Entry** drop-down arrow and choose an entry from the menu. The Cisco VPN Client then uses this DUN entry to automatically dial into the Microsoft network before making the VPN connection to the private network.

■ Third-party dial-up application—If you have no DUN phonebook entries and have enabled the Connect to Internet via dial-up feature, then the third-party dial-up application is enabled by default. Click **Browse** to enter the name of the program in the Application field. This application launches the connection to the Internet. The string you enter in this field is the path name to the command that starts the application and the name of the command. For example: c:\isp\ispdialer.exe dialEngineering would activate the ispdialer using the script "dialEngineering," which would contain the required dial information.

Working with the Cisco VPN Client

This topic contains information regarding the Cisco VPN Client program menus, log viewer, and status displays.
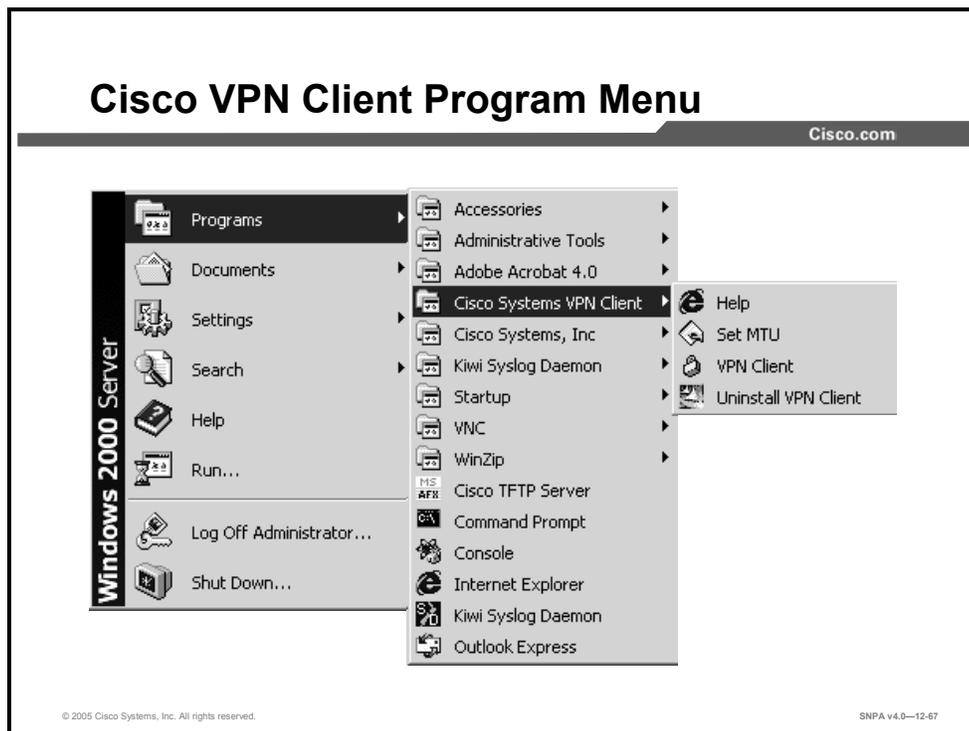
This figure displays the Cisco VPN Client program menu as viewed on a Windows 2000 PC.

After the VPN Software Client has been installed, access the VPN Software Client program menu by choosing **Start > Programs > Cisco Systems VPN Client**. Under the Cisco Systems VPN Client menu, a number of options are available:

■ Help—Accesses Software Client help text. Help is also available by doing the following:

— Press **F1** at any window while using the Cisco VPN Client.

— Click the **Help** button on windows that display it.

— Click the logo in the title bar.

■ Set MTU—The Software Client automatically sets the maximum transmission unit (MTU) size to approximately 1420 bytes. For specific applications, Set MTU can change the MTU size to fit a specific scenario.

■ Uninstall VPN Client—Only one VPN Software Client can be loaded at a time. When you are upgrading, you must uninstall the old VPN Software Client before installing the new VPN Software Client. Choose **Uninstall VPN Client** to remove the old VPN Software Client.

Virtual Adapter

SNPA v4.0—12-68
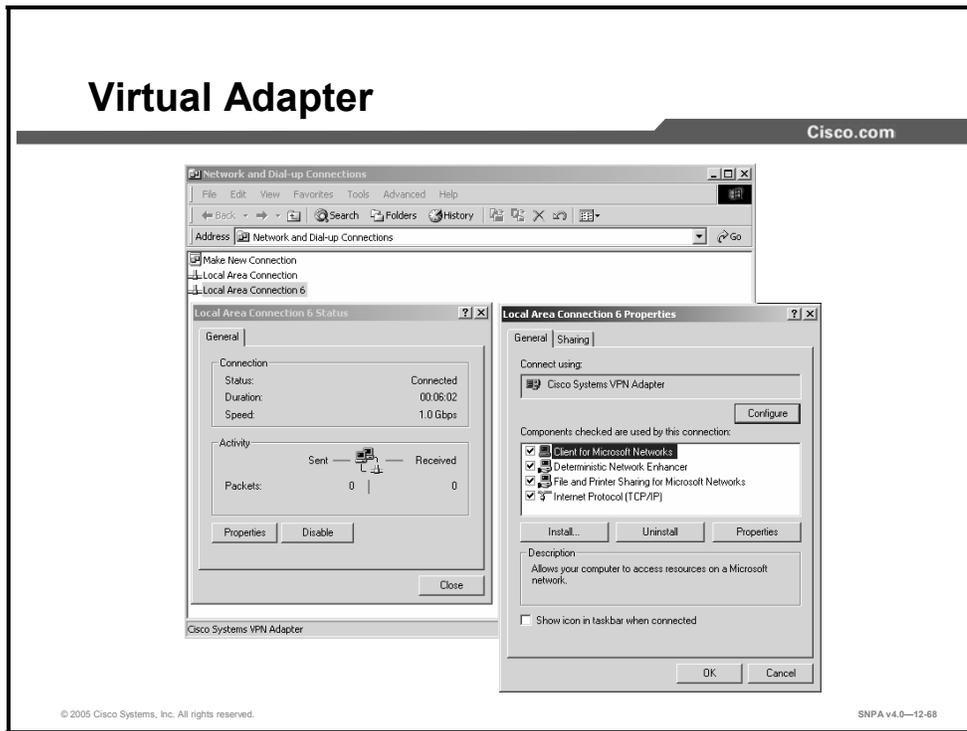
A virtual adapter is a software-only driver that acts as a valid interface in the system. Its purpose is to solve protocol incompatibility problems. The virtual adapter appears in the network properties list just like a physical adapter and displays all the information you would usually find under any other network adapter that is installed. It is available on Windows 2000 and XP only.

Setting MTU Size

Cisco Systems SetMTU

CAUTION: MTU changes can affect your PC's performance on the network.

Network Adapters (IPSec only)

- Dial-up Networking
- Local Area Connection
- Local Area Connection 2

MTU Options

○ Default   ○ 576   ● 1300   ○ Custom   `1300`

[OK]   [Cancel]   [Help]

SNPA v4.0—12-69
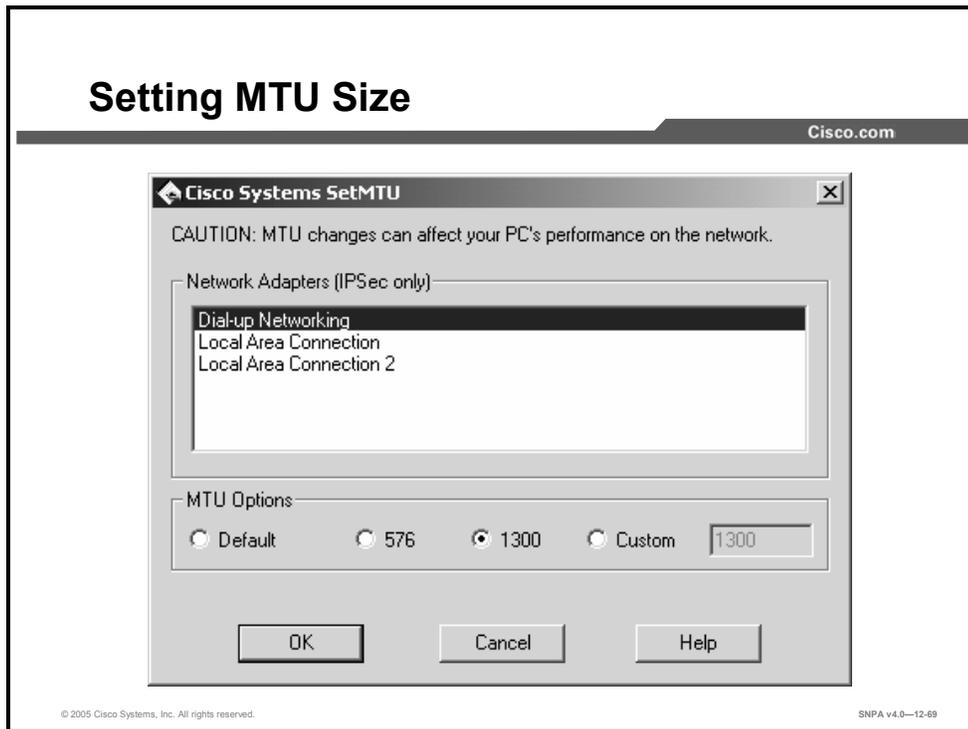
This figure displays the SetMTU window, which is where you set the MTU size.

The Set MTU option is used primarily for troubleshooting connectivity problems. For specific applications where fragmentation is still an issue, Set MTU can change the MTU size to fit the specific scenario. The Cisco VPN Client automatically adjusts the MTU size to suit your environment, so running this application should not be necessary.

To implement a different MTU size, select the network adapter in the Network Adapters (IPSec only) field. In the example in the figure, Dial-up Networking is selected. In the MTU Options group box, set the MTU option size by clicking the appropriate radio button. You must reboot for MTU changes to take effect.

Cisco VPN Client Statistics Menu

SNPA v4.0—12-70
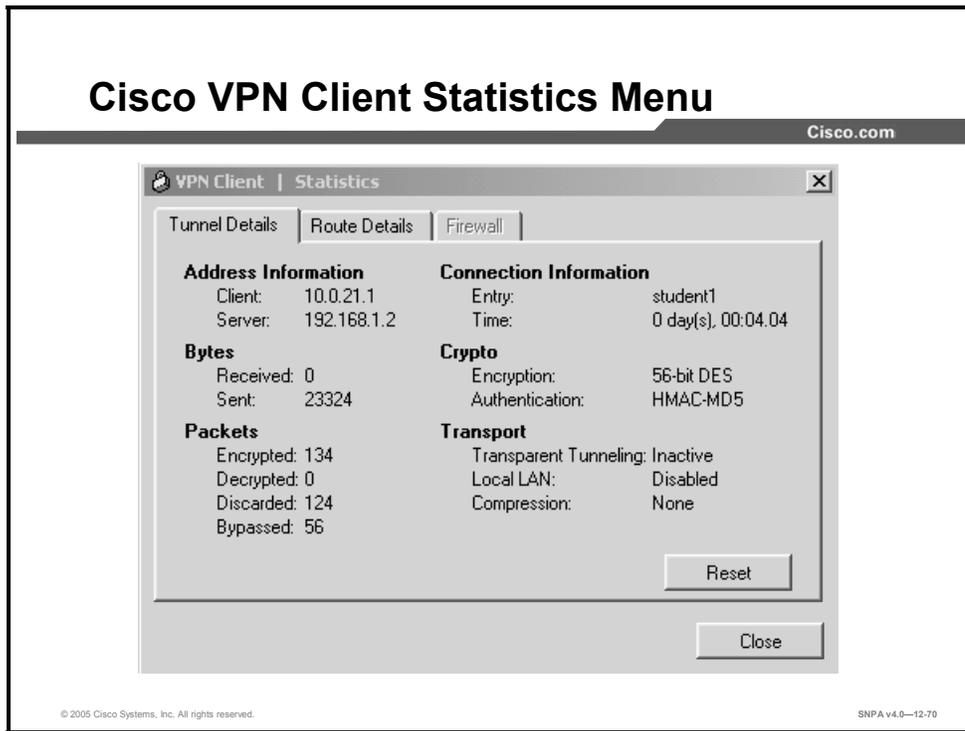
The Cisco VPN Client Statistics menu provides information regarding the current status of the VPN connection. Three tabs contain details on the tunnel, route, and firewall parameters in use.

Summary

This topic summarizes what you have learned in this lesson.

Summary

Cisco.com

- **Cisco Easy VPN features greatly enhance deployment of remote access solutions for Cisco IOS software customers.**
- **The Easy VPN Server adds several new commands to Cisco PIX Firewall Security Appliance Software v6.3 and later versions.**
- **The Cisco VPN Client enables software-based VPN remote access.**

SNPA v4.0—12-71

Lesson 13

Configuring ASA for WebVPN

Overview

This lesson begins by defining the characteristics of WebVPN and how it compares with traditional virtual private networks (VPNs). The end-user interface is then presented along with the steps and commands necessary to configure the Cisco ASA 5500 Series Adaptive Security Appliance (ASA) for WebVPN.

Objectives

Upon completing this lesson, you will be able to configure the ASA to support the WebVPN feature set. This includes being able to meet these objectives:

- Explain the purpose of WebVPN
- Describe the WebVPN end-user interface
- Configure WebVPN general parameters
- Configure WebVPN servers and URLs
- Configure WebVPN port forwarding
- Define e-mail proxy servers
- Configure WebVPN content filters and ACLs

WebVPN Feature Overview

WebVPN lets users establish a secure, remote access VPN tunnel to an ASA using a web browser. Users are no longer "tethered" to a particular PC or workstation, improving mobility and flexibility of access.

WebVPN Overview

WebVPN (SSL VPN) complements IPSec-based remote access by allowing secure remote access to corporate network resources without the use of VPN Client software.

SNPA v4.0—13-3

There is no need for either a software or hardware client (IPSec or Point-to-Point Tunneling Protocol [PPTP]-based). WebVPN provides easy access to a broad range of enterprise applications, including web resources, web-enabled applications, Windows NT/Active Directory file shares (web enabled), e-mail, and other TCP-based applications from any computer connected to the Internet that can reach Hypertext Transfer Protocol (HTTP) and HTTP secure (HTTPS) Internet sites.

WebVPN uses Secure Socket Layer (SSL) protocol and its successor, Transport Layer Security (TLS) protocol, to provide a secure connection between remote users and specific, supported internal resources at a central site.

WebVPN Features
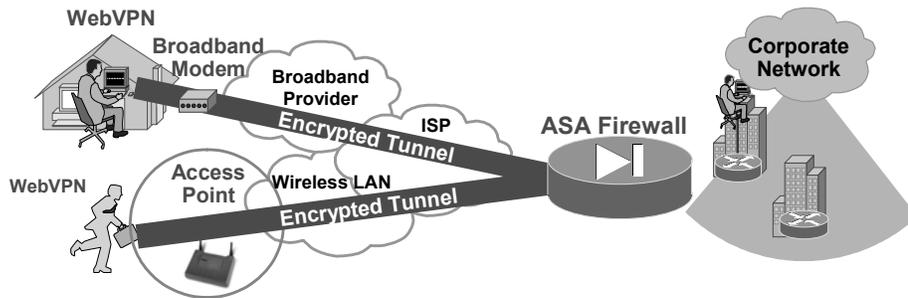
- **Access to internal websites (HTTP/HTTPS), including filtering**
- **Access to internal Windows (CIFS) File Shares**
- **TCP port forwarding for legacy application support**
- **Access to e-mail via POP, SMTP, and IMAP4 over SSL**

SNPA v4.0—13-4

WebVPN features include the following:

- Secure access to internal websites via HTTPS

- Access, through Windows File Access, to files on preconfigured file servers or via file browsing on the network

- Port forwarding (application access) for legacy application support

- E-mail proxies that enable e-mail via Post Office Protocol v3 secure (POP3S) over SSL, Internet Message Access Protocol v4 secure (IMAP4S) over SSL, and Simple Mail Transfer Protocol secure (SMTPS) over SSL proxies

- Messaging application programming interface (MAPI) proxy support for Microsoft Exchange

- Support for popular web e-mail applications, including Microsoft Outlook Web Access (OWA) and Lotus iNotes

WebVPN is ideal for the following deployments:

- Unmanaged desktops

   — Extranets

   — Employee-owned computers

- "Lite" users

   — Employees who need only occasional access

   — Employees who need access to few applications

- Simple or locked-down access

   — Restricted server and application access by population

WebVPN and IPSec Comparision

Cisco.com

WebVPN	IPSec VPN
• Uses a standard web browser to access the corporate network	• Uses purpose-built client software for network access
• SSL encryption native to browser provides transport security	• Client provides encryption and desktop security
• Applications accessed through browser portal	• Client establishes seamless connection to network
• Limited client/server applications accessed using applets	• All applications are accessible through their native interface

SNPA v4.0—13-5

Each type of remote access has its own unique set of benefits. WebVPN allows "clientless" access, but there are possible trade-offs in ease of use and security. Many of these trade-offs can be mitigated by properly implementing WebVPN. Note the following additional characteristics of each solution:

■ WebVPN—Using a web browser for remote access enables:

— Anywhere access

— Access from noncorporate machines

— Customized user portals

— Easy firewall traversal from any location

■ IPSec VPN—Using an IPSec client for remote access enables:

— Access to any application

— Native application interfaces

— Consistent user experience

— Embedded security, such as a personal firewall

WebVPN End-User Interface

This topic describes the end-user interface provided by WebVPN.
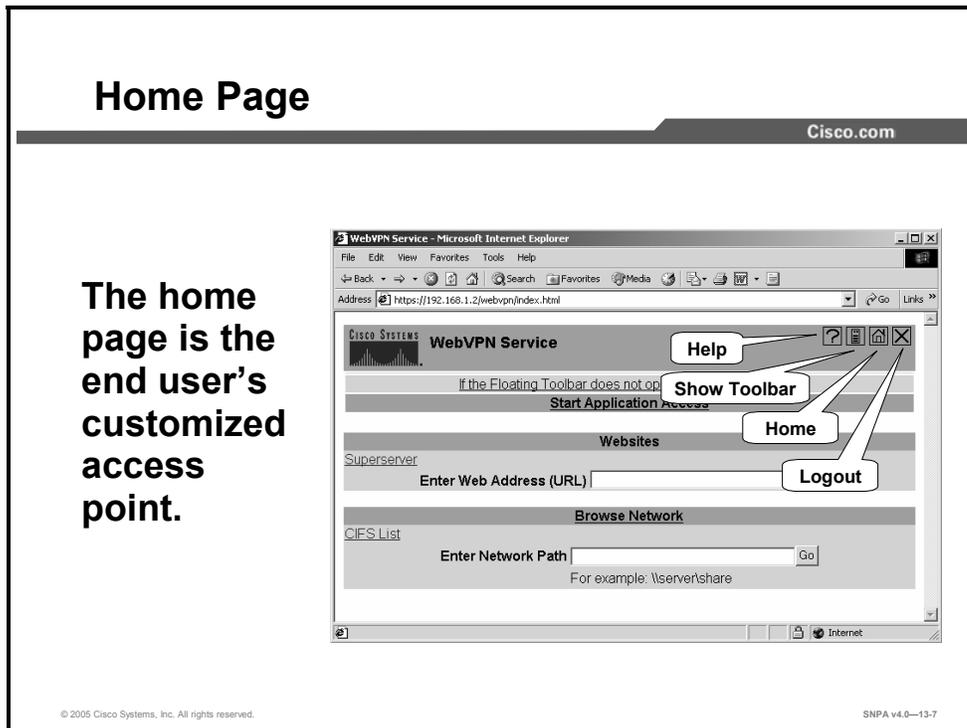
The administrator designs this page to meet the requirements of individual end users. Using this interface, the end user can conveniently and securely access the organization's internal network from any computer that has an Internet connection. The end user can check e-mail, view or transfer files, visit internal corporate websites, and run internal web applications from any web browser. The user navigates using the buttons provided within the WebVPN interface window. The following buttons are available:

■ Help—Click this icon to access this help system.

■ Show Toolbar—Click this icon to show the WebVPN toolbar.

■ Home—Click this icon to return to your home page.

■ Logout—Click this icon to end your remote access session.

Website Access and Browsing Files

SNPA v4.0—13-8
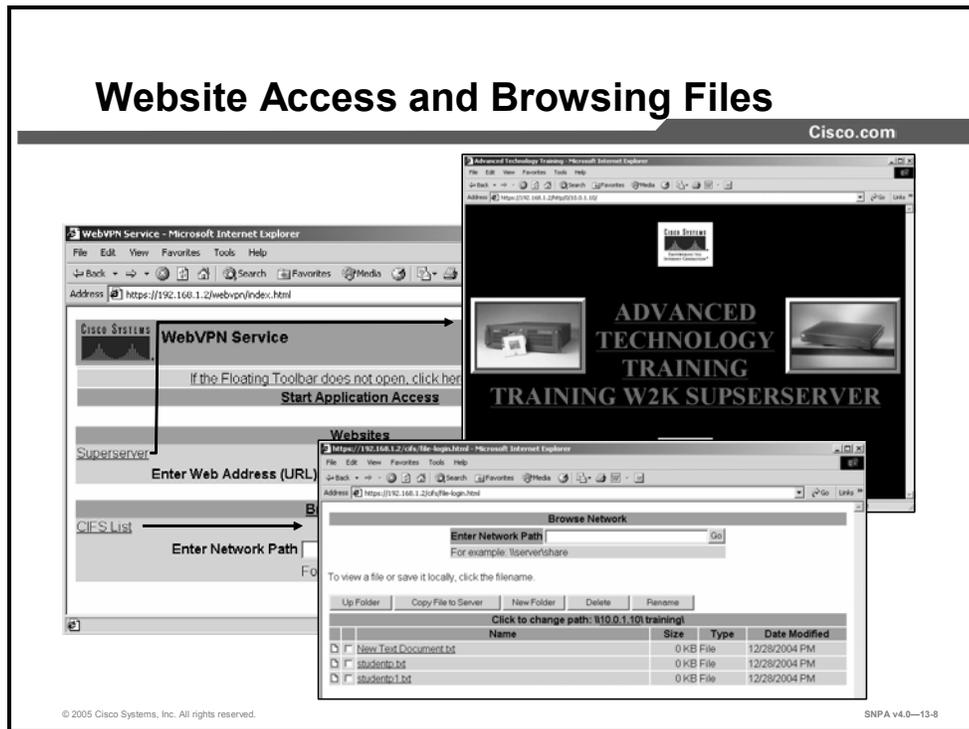
If the administrator sets up end-user accounts to access particular websites or file shares, one or more links appear under Websites on the end user's home page. To access the website or file share, the end user simply clicks the link. If the site is protected, the end user will have to enter a username and password.

If the administrator has granted end-user access to a server that is not specifically listed, the end user can enter the web address of the server directly into the Enter Web Address (URL) text box or the Enter Network Path text box. Alternately, the end user can browse the network by clicking the Browse Network link.

After end users are connected to a file share, they can upload and download files, create new folders, and delete and rename files.

Whenever the end user is visiting a website via a secure remote access session, a toolbar appears on the web page. The toolbar is to remind the end user that the access is being provided through the corporate network and for navigation purposes.

Port Forwarding

Cisco.com

© 2005 Cisco Systems, Inc. All rights reserved.   SNPA v4.0—13-9
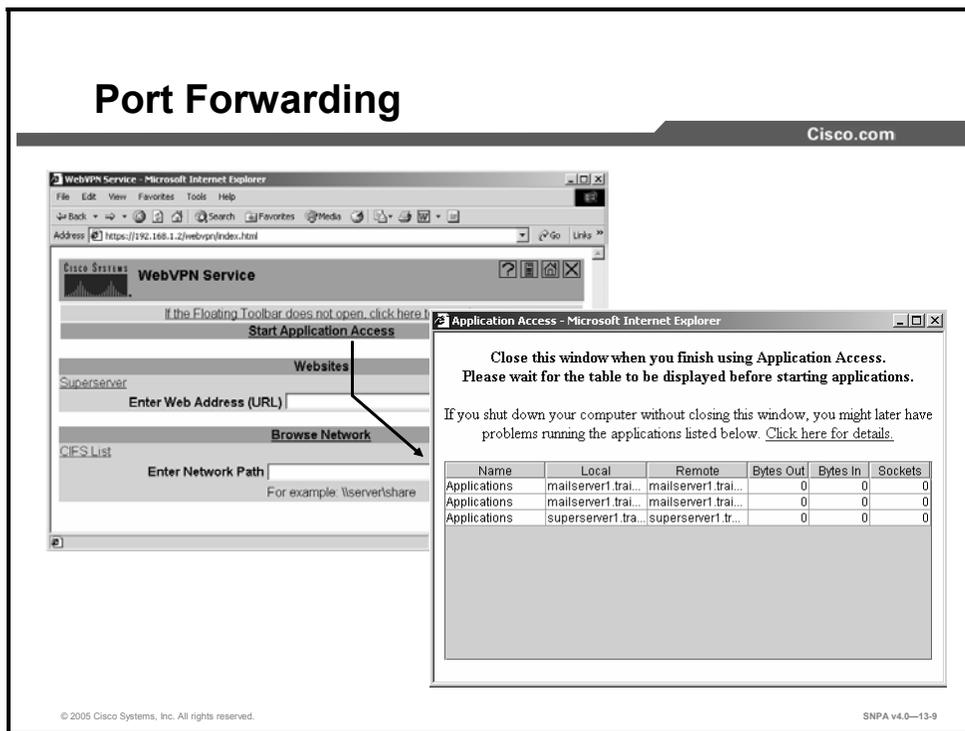
The administrator can configure certain client-server applications for the end user's use. Start Application Access (port forwarding) opens a secure connection between the end-user computer and the remote server. When the window is open or minimized, the connection is active; if the end user quits the window, the connection closes.

Note	Port forwarding requires Sun Microsystems Java™ Runtime Environment v1.4.1 (1.5.or later preferred) to be installed on your system. It can be downloaded automatically if needed.

The chart in the Application Access window lists the available applications and key details about the secure connection. This chart is display only. The end user cannot edit it, and clicking on a cell does not start the application.

WebVPN provides access to TCP-based applications by mapping application-specific ports on the end user's PC to application-specific ports on servers behind the ASA. When an end user accesses an application over WebVPN using hostnames to identify the application server, the ASA modifies the Windows Hosts file to include a mapping entry for that application.

The chart has the following fields:

- Name—The name of an available client application

- Local—The hostname (or IP address) and TCP port to configure on the client application to allow communication with the remote server

- Remote—The hostname (or IP address) and TCP port of the remote server

- Bytes In/Out—The amount of data that this application receives or sends through the secure connection

- Sockets—The number of TCP connections that the application is using

Caution	A warning for Microsoft Windows users: Always close the Port Forwarding window when you finish using the client/server applications. If you shut down your computer without closing this window, you might later have problems running these applications. You also might be unable to access the application's host (such as your mail server).

Configure WebVPN General Parameters

This topic describes the general WebVPN parameters that are present and configurable.

Enabling the HTTP Server

Cisco.com

- **The HTTP server must be enabled.**
- **ASDM and WebVPN cannot be run on the same interface.**

firewall(config)#

```
http server enable
```

- **Enables the HTTP server for WebVPN**

```
fw1(config)# http server enable
```

SNPA v4.0—13-11

WebVPN uses the internal HTTP server. To enable the HTTP server, use the **http server enable** command. It is not permitted to have both Cisco Adaptive Security Device Manager (ASDM) and WebVPN enabled on the same interface. Users will receive an error if ASDM has already been configured on the interface.

WebVPN Subcommand Mode

The WebVPN subcommand mode configures general WebVPN parameters and the look and feel of the end-user interface. The following items can be configured:

- **accounting-server-group**
- **authentication**
- **authentication-server-group**
- **authorization-dn-attributes**
- **authorization-required**
- **authorization-server-group**
- **accounting-server-group**
- **authentication**
- **authorization-server-group**
- **default-group-policy**
- **default-idle-timeout**
- **enable**
- **http-proxy**

- **https-proxy**
- **login-message**
- **Logo**
- **Logout-message**
- **nbns-server**
- **password-prompt**
- **secondary-color**
- **secondary-text-color**
- **text-color**
- **title**
- **title-color**
- **username-prompt**

```
fw1(config)# webvpn
fw1(config-webvpn)#
```

SNPA v4.0—13-12

The items listed in the slide are configured in one location and apply to all users accessing the security appliance via WebVPN. Generally, they apply to items where the group has not been determined. This configuration is done using the webvpn subcommand mode. The **webvpn** command is used to enter the subcommand mode. WebVPN does not need to be configured for the e-mail proxies to be configured.

These **webvpn** commands let you configure AAA servers, default group policies, default idle timeout, HTTP and HTTPS proxies, and NetBIOS Name Service (NBNS) servers for WebVPN as well as the appearance of WebVPN screens that end users see.

Enabling WebVPN Interfaces

- **WebVPN initially needs to be enabled on each interface that will have WebVPN users.**
- **ASDM and WebVPN cannot be enabled on the same interface.**
- **A DNS server must be configured for WebVPN and MAPI to function.**

```
firewall(config-webvpn)#
```

```
 enable ifname
```

```
fw1(config)# webvpn
fw1(config-webvpn)# enable outside
```

```
fw1(config)# pop3s
fw1(config-pop3s)# enable outside
```

SNPA v4.0—13-13

To enable WebVPN or e-mail proxy access on a previously configured interface, use the **enable** command. For WebVPN, use this command in webvpn mode. For e-mail proxies (IMAP4S, POP3S, SMTPS), use this command in the applicable e-mail proxy mode. To disable WebVPN on an interface, use the **no** version of the command.

NBNS Server Configuration

Remote Client

NBNS Server

WebVPN Tunnel

ASA
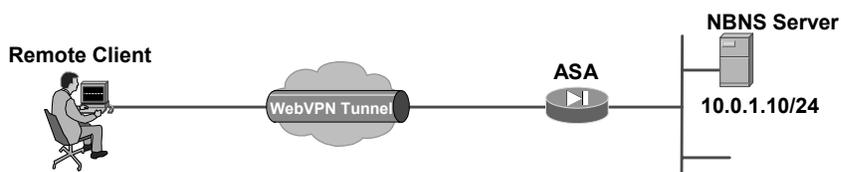
10.0.1.10/24

```
firewall(config-webvpn)#
```

```
nbns-server {ipaddr or hostname} [master] [timeout
timeout] [retry retries]
```

• **Enables NetBIOS resolution for CIFS File Shares.**

```
fw1(config-webvpn)# nbns-server 10.0.1.10
```

SNPA v4.0—13-14

The security appliance queries NBNS servers to map NetBIOS names to IP addresses. WebVPN requires NetBIOS to access or share files on remote systems. There is a maximum of three server entries. The first server that is configured is the primary server, and the others are backups for redundancy.

The **nbns-server** command adds an NBNS\ server for Common Internet File System (CIFS) name resolution. Specifying the **master** option indicates that this is a master browser, rather than just a Windows Internet Name Service (WINS) server. This command may be entered multiple times. The **no** option will remove the matching entry from the configuration. The timeout value is in seconds. The default timeout value is 2 seconds; the range is 1 to 30. The default number of retries is 2; the range is 0 to 10.

The syntax for the **nbns-server** command is as follows:

```
nbns-server {ipaddr or hostname} [master] [timeout timeout]
[retry retries]
```

hostname	Specifies the hostname for the NBNS server.
ipaddr	Specifies the IP address for the NBNS server.
master	Indicates that this is a master browser, rather than a WINS server.
retry	Indicates that a retry value follows.
retries	Specifies the number of times to retry queries to NBNS servers. The security appliance recycles through the list of servers the number of times you specify here before sending an error message. The default value is 2; the range is 1 to 10.
timeout	Indicates that a timeout value follows.
timeout	Specifies the amount of time that the security appliance waits before sending the query again, to the same server if there is only one, or another server if there are multiple NBNS servers. The default timeout is 2 seconds; the range is 1 to 30 seconds.

Authentication Server Configuration

ACS Server

Remote Client

Security Appliance

WebVPN Tunnel

10.0.1.10/24
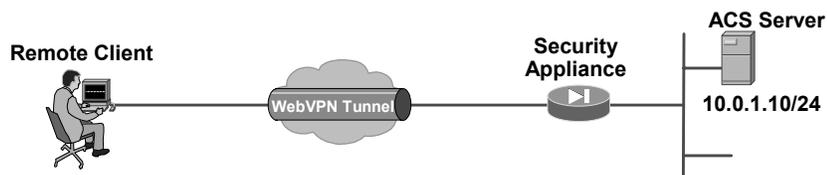
firewall(config-webvpn)#

```
authentication-server-group group tag
```

- **Specifies the authorization server that WebVPN users should use.**
- **Authorization server must be previously configured using** aaa-server **commands**

```
fw1(config-webvpn)# authentication-server-group
  AUTHSERVER
```

SNPA v4.0—13-15

The **authentication-server-group** command specifies the set of authentication servers to use with WebVPN or one of the e-mail proxies. For WebVPN, use this command in webvpn mode. For e-mail proxies (IMAP4S, POP3S, or SMTPS), use this command in the applicable e-mail proxy mode. The default is to not have any authentication servers configured.

Home Page Look and Feel Configuration
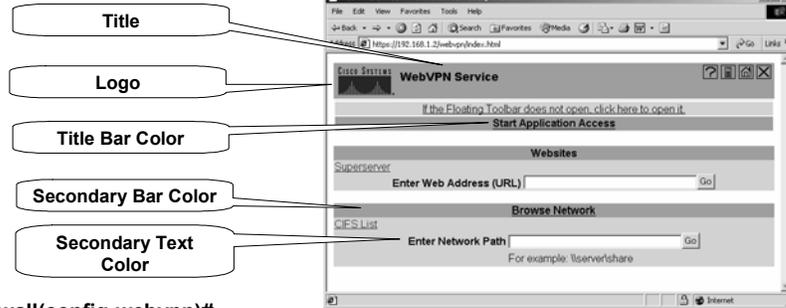
firewall(config-webvpn)#

```
title titletext
```

- **Specifies the title that WebVPN users should see.**

firewall(config-webvpn)#

```
title-color color
```

- **Specifies the title color. Supported formats include HTML color name string, HTML color value, and HTML RGB value.**

SNPA v4.0—13-16

Many of the commands in the webvpn subcommand mode control and customize the look and feel of the end user's home page. Some of the items that can be configured include:

- HTML title—The HTML title string that is in the browser title and on the title bar; is limited to 255 characters. The default is WebVPN Service. Specifying no title removes the command from the configuration and resets the value to the default. To have no title, the **title** command is issued without a string.

- Login message—This is the HTML text that prompts the user to log in; is limited to 255 characters. The default is "Please enter your username and password." This string is presented to the user before login. Specifying no login message removes the command from the configuration and resets the value to the default. To have no login message, the **login-message** command is issued without a string.

- Logo—This is the custom logo image that is displayed on the login and home pages. It is a file that can be uploaded by the administrator to the security gateway. The filename is limited to a legal filename length (no more than 255 characters). The logo must be a JPG, PNG or GIF file and must be less than 100 KB. An error will occur if the file does not exist. If the logo file is subsequently deleted, then no logo is displayed. The default is to use the Cisco Systems logo. Specifying no logo removes the command from the configuration and resets the value to the default. To have no logo, specify **logo none**.

- Title color—This is the color of the title bars on the login, home and file access pages. The value can be a comma-separated RGB value, an HTML color value (beginning with a "#"), or the name of the color that is recognized in HTML. The value is limited to 32 characters. The default is one of the Cisco purples (#9999CC). Specifying **no title-color** reverts the value to the default.

- Secondary color—This is the color of the secondary title bars on the login, home and file access pages. The value can be a comma-separated RGB value, an HTML color value (beginning with a "#"), or the name of the color that is recognized in HTML. The value is limited to 32. The default is one of the Cisco purples (#CCCCFF). Specifying **no secondary-color** reverts the value to the default.

- Text color—This is the color of the text on the title bars. It is restricted to just two values to limit the number of icons that need to exist for the toolbar. The default value is white. Specifying **no text-color** reverts the value to the default.

- Secondary text color—This is the color of the text on the secondary bars. It is restricted to be aligned with the title bar text color. The default value is black. Specifying **no secondary-text-color** reverts the value to the default.

Configure WebVPN Servers and URLs

This topic covers how to configure WebVPN servers and URLs.

Enable WebVPN Protocol for Group Policy
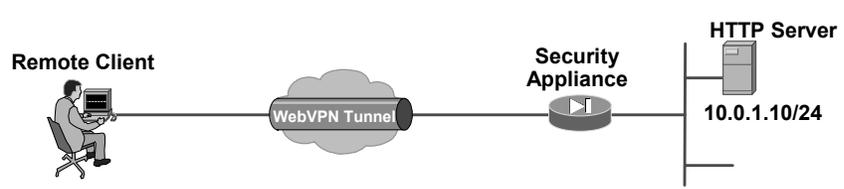
Remote Client

WebVPN Tunnel

Security Appliance

HTTP Server

10.0.1.10/24

firewall(config)#

```
group-policy {name} attributes
```

- **Enters the group-policy attributes subcommand mode**

```
fw1(config)# group-policy WEBVPN1 attributes
```

firewall(config-group-policy)#

```
vpn-tunnel-protocol {webvpn | IPSec}
```

- **Enables WebVPN for group**

```
fw1(config-group-policy)# vpn-tunnel-protocol webvpn
```

SNPA v4.0—13-18

Use the **vpn-tunnel-protocol** command in group-policy configuration mode or username configuration mode to configure a VPN tunnel type (IPSec or WebVPN) for the user or group. The following types are available:

- **IPSec**—Negotiates an IPSec tunnel between two peers (a remote access client or another secure gateway). Creates security associations (SAs) that govern authentication, encryption, encapsulation, and key management.

- **webvpn**—Provides VPN services to remote users via an HTTPS-enabled web browser and does not require a client.

Enable URL Entry for WebVPN Users
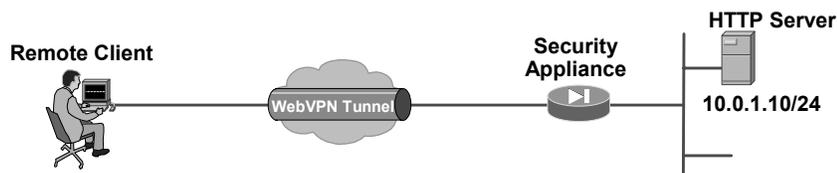
Cisco.com

HTTP Server

Remote Client

Security Appliance

WebVPN Tunnel

10.0.1.10/24

firewall(config)#

```
group-policy {name} attributes
```

- **Enters the group-policy attributes subcommand mode**

```
fw1(config)# group-policy WEBVPN1 attributes
```

firewall(config-group-policy)#

```
webvpn
```

- **Enters WebVPN group-policy attributes subcommand mode**

```
fw1(config-group-policy)# webvpn
```

SNPA v4.0—13-19

Use the **webvpn** command in group-policy configuration mode or in username configuration mode to enter the webvpn subcommand mode. These **webvpn** commands apply to the username or group policy from which you configure them. **webvpn** commands for group policies and usernames define access to files, MAPI proxies, URLs and TCP applications over WebVPN. They also identify access control lists (ACLs) and types of traffic to filter.

Webvpn mode, which you enter from global configuration mode, lets you configure global settings for WebVPN. Webvpn mode, which you enter from group-policy or username mode, lets you customize a WebVPN configuration for specific users or group policies. You do not need to configure WebVPN to use e-mail proxies.

Enable URL Entry for WebVPN Users (Cont.)
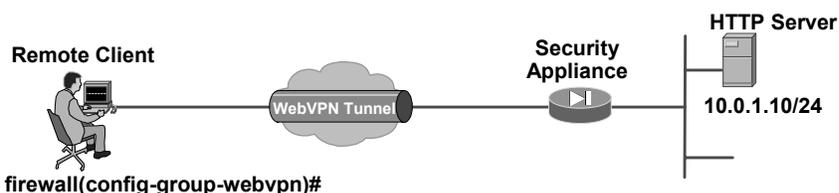
HTTP Server

Remote Client

Security Appliance

WebVPN Tunnel

10.0.1.10/24

firewall(config-group-webvpn)#

```
functions {file-access | file-browsing | file-entry |
  filter | url-entry | mapi | port-forward | none}
```

• **Enables file access, entry, browsing, and URL entry for the group**

```
fw1(config-group-webvpn)# functions url-entry file-access
  file-entry file-browsing
```

firewall(config-group-webvpn)#

```
url-list {value name | none}
```

• **Selects predefined URLs that were configured by using the** url-list **command**

```
fw1(config-group-webvpn)# url-list value URLs
```

SNPA v4.0—13-20

Use the **functions** command in webvpn mode to enable file access and file browsing, MAPI proxies, and URL entry over WebVPN for this user or group policy. To remove a configured function, use the **no** form of this command. To remove all configured functions, including a null value created by issuing the **functions none** command, use the **no** form of this command without arguments. The **no** option allows inheritance of a value from another group policy. To prevent inheriting function values, use the **functions none** command. Functions are disabled by default.

The **url-entry** parameter enables or disables user entry of URLs. When enabled, the security appliance still restricts URLs with any configured URL or network ACLs. When URL entry is disabled, the security appliance restricts WebVPN users to the URLs on the home page.

Use the **url-list** command in webvpn mode to apply a list of WebVPN servers and URLs to a particular user or group policy, which you enter from group-policy or username mode. To remove a list, including a null value created by using the **url-list none command,** use the **no** form of this command. The **no** option allows inheritance of a value from another group policy. To prevent inheriting a URL list, use the **url-list none** command.

Before you can use the **url-list** command in webvpn mode to identify a URL list that you want to display on the WebVPN home page for a user or group policy, you must create the list. Use the **url-lis**t command in global configuration mode to create one or more lists.

The syntax for the **functions** command is as follows:

```
functions {file-access | file-browsing | file-entry | filter |
url-entry | mapi | port-forward | none}
```

file-access	Enables or disables file access. When enabled, the WebVPN home page lists file servers in the server list. You must enable file access to enable file browsing and file entry.
file-browsing	Enables or disables browsing for file servers and shares. You must enable file browsing to allow user entry of a file server.
file-entry	Enables or disables user ability to enter names of file servers.
filter	Applies a web-type ACL. When enabled, the security appliance applies the web-type ACL defined with the **webvpn filter** command.
mapi	Enables or disables Microsoft Outlook/Exchange port forwarding.
none	Sets a null value for all WebVPN functions. Prevents inheriting functions from a default or specified group policy.
port-forward	Enables port forwarding. When enabled, the security appliance uses the port forwarding list that is defined with the **webvpn port-forward** command.
url-entry	Enables or disables user entry of URLs. When enabled, the security appliance still restricts URLs with any configured URL or network ACLs. When URL entry is disabled, the security appliance restricts WebVPN users to the URLs on the home page.

The syntax for the **url-list** command is as follows:

```
url-list {value name | none}
```

value *name*	Specifies the name of a previously configured list of URLs. To configure such a list, use the **url-list** command in global configuration mode.
none	Sets a null value for URL lists. Prevents inheriting a list from a default or specified group policy.

url-list Command

Remote Client

Security Appliance

Superserver

WebVPN Tunnel

10.0.1.10/24
Cisco Training

10.0.1.11/24

Websites

Superserver
Enter Web Address (URL) [Go]

Browse Network

CIFS Share
Enter Network Path [Go]
For example \\server\share
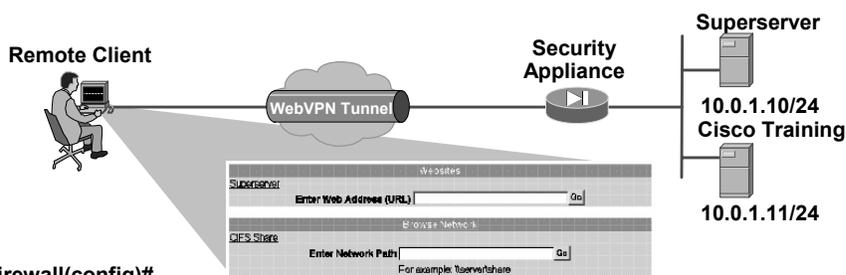
firewall(config)#

```
url-list {listname displayname url}
```

- **Defines the name of the URL list**
- **Defines the text the users see for the link on their home page**
- **Defines the actual URL that the link accesses**
- **List of WebVPN links can be HTTP, HTTPS, and CIFS servers**

```
fw1(config)# url-list URLs "Superserver" http://10.0.1.10
fw1(config)# url-list URLs "CIFS Share" cifs://10.0.1.11/training
```

SNPA v4.0—13-21

Use the **url-list** command in global configuration mode to configure a set of URLs for WebVPN users to access. To configure a list with multiple URLs, use this command with the same *listname* multiple times, once for each URL. To remove an entire configured list, use the **no url-list** *listname* command. To remove a configured URL, use the **no url-list** *listname url* command. To configure multiple lists, use this command multiple times, assigning a unique *listname* to each list.

You use the **url-list** command in global configuration mode to create one or more lists of URLs. To allow access to the URLs in a list for a specific group policy or user, use the *listname* you create here with the **url-list** command in webvpn mode.

The syntax for the **url-list** command is as follows:

```
url-list {listname displayname url}
```

displayname	Provides the text that displays on the WebVPN end-user interface to identify the URL. Maximum 64 characters. The *displayname* must be unique for a given list. Spaces are allowed.
listname	Groups the set of URLs that WebVPN users can access. Maximum 64 characters. Semicolons (;) ampersands (&), and less-than (<) characters are not allowed.
url	Specifies the link. Supported URL types are HTTP, HTTPS, and CIFS.

Example: Servers and URL Configuration

Security Appliance

Superserver/CIFS Share

192.168.1.0

10.0.1.0

.5   .5   .10
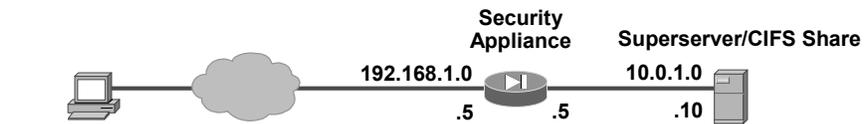
WebVPN Client
172.26.26.1

Web access Security Appliance parameters:
- **Example—**url-list URLs "Superserver" http://10.0.1.10

WebVPN client parameters:
- **Need to launch WebVPN interface**
- **Click on Superserver or CIFS Share link**

CIFS access Security Appliance parameters:
- **Example—**url-list URLs "CIFS Share" cifs://10.0.1.10/training

SNPA v4.0—13-22

This example illustrates the various parameters that must be configured on the security appliance to enable WebVPN access to the resources on the private network. File access via CIFS is configured in the same basic manner.

Configure WebVPN Port Forwarding

This topic covers how to configure WebVPN port forwarding.

Enable Port Forwarding for WebVPN Users

Cisco.com
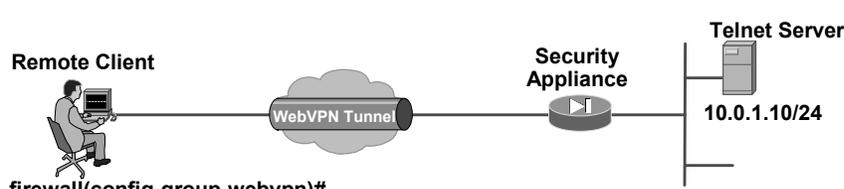
Remote Client — WebVPN Tunnel — **Security Appliance** — **Telnet Server** 10.0.1.10/24

`firewall(config-group-webvpn)#`

```
functions {file-access | file-browsing | file-entry |
   filter | url-entry | mapi | port-forward | none}
```

• **Enables port forwarding for the group**

```
fw1(config-group-webvpn)# functions port-forward
```

`firewall(config-group-webvpn)#`

```
port-forward {value listname | none}
```

• **Enters predefined port forwarding list configured by using the** port-forward **command**

```
fw1(config-group-webvpn)# port-forward value Applications
```

© 2005 Cisco Systems, Inc. All rights reserved. SNPA v4.0—13-24

Use the **port-forward** command in webvpn mode to enable WebVPN application access for this user or group policy. To remove the port forwarding attribute from the configuration, including a null value created by issuing the **port-forward none** command, use the **no** form of this command. The **no** option allows inheritance of a list from another group policy. To prevent inheriting a port forwarding list, use the **port-forward none** command.

The *listname* value identifies the list of applications that WebVPN users can access. Before you can use the **port-forward** command in webvpn mode to enable application access, you must define a list of applications that you want users to be able to use in a WebVPN connection. Use the **port-forward** command in global configuration mode to define this list.

port-forward Command
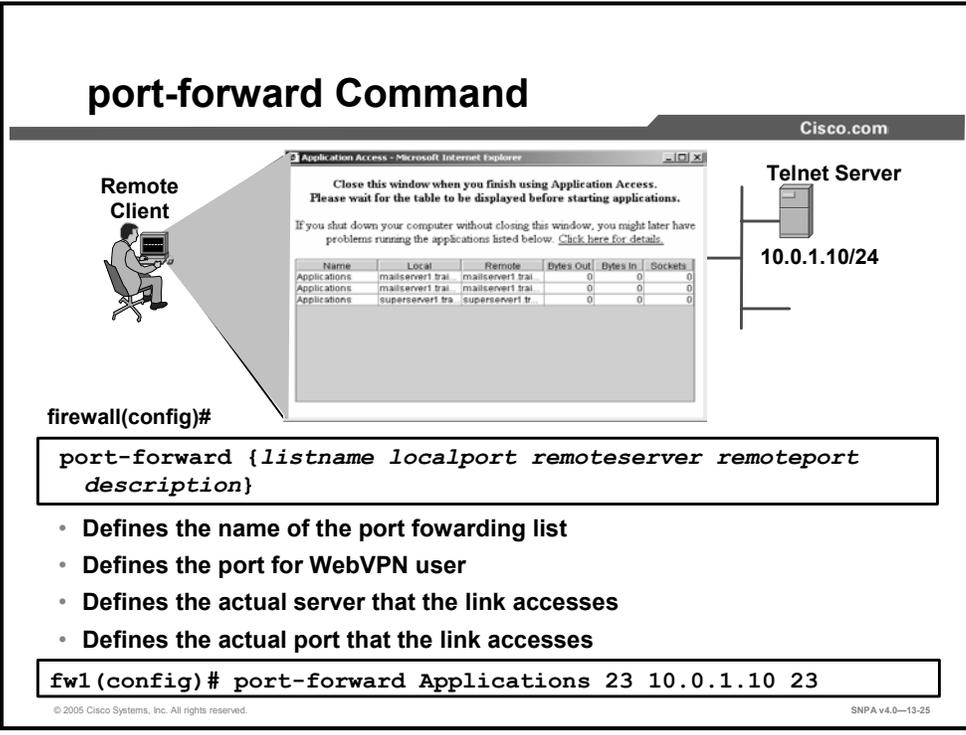
Remote Client

Telnet Server

10.0.1.10/24

Application Access - Microsoft Internet Explorer

**Close this window when you finish using Application Access.
Please wait for the table to be displayed before starting applications.**

If you shut down your computer without closing this window, you might later have
problems running the applications listed below. Click here for details.

Name	Local	Remote	Bytes Out	Bytes In	Sockets
Applications	mailserver1 trai...	mailserver1 trai...	0	0	0
Applications	mailserver1 trai...	mailserver1 trai...	0	0	0
Applications	superserver1 tra...	superserver1 tr...	0	0	0

firewall(config)#

```
port-forward {listname localport remoteserver remoteport
  description}
```

• **Defines the name of the port fowarding list**
• **Defines the port for WebVPN user**
• **Defines the actual server that the link accesses**
• **Defines the actual port that the link accesses**

```
fw1(config)# port-forward Applications 23 10.0.1.10 23
```

With port forwarding, you provide mapping information that the security appliance adds to the host's file on a user's PC as the application opens. This mapping information lets the PC connect to the server at the central site that supports the desired application.

Port forwarding can work only if the applications on remote servers are uniquely identified, and therefore reachable, either by hostname or by IP address and port. Keep the following in mind when configuring port forwarding:

■ Hostnames, correctly defined on the security appliance, are constant and are by definition unique.

Note   The use of hostnames is recommended.

■ IP addresses change depending on the end user's location relative to the remote server. If you identify the remote server by IP address, users must reconfigure the application on their PC each time they change location.

Use the **port-forward** command in global configuration mode to configure the set of applications that WebVPN users can access over forwarded TCP ports. To configure access to multiple applications, use this command with the same *listname* multiple times, once for each application. To remove an entire configured list, use the **no port-forward** *listname* command. To remove a configured application, use the **no port-forward** *listname localport* command (you need not include the *remoteserver* and *remoteport* parameters).

To allow access to particular TCP port forwarding applications for a specific user or group policy, use the *listname* you create here with the **port-forward** command in webvpn mode.

The syntax for the **port-forward** command is as follows:

```
port-forward {listname localport remoteserver remoteport
description}
```

listname	Groups the set of applications (forwarded TCP ports) that WebVPN users can access. Maximum 64 characters.
localport	Specifies the local port that listens for TCP traffic for an application. You can use a local port number only once for a *listname*. To avoid conflicts with local TCP services, use port numbers in the range of 1024 to 65535.
remoteserver	Provides the Domain Name System (DNS) name or IP address of the remote server for an application. We recommend using DNS names.
remoteport	Specifies the port on the remote server to which this application will connect.
description	Provides the application name or short description that displays on the end user's port forwarding Java applet screen. Maximum 64 characters.

Port Forwarding Configuration Example: DNS Versus IP Address

Security Appliance

Telnet Server—Training

192.168.1.0

10.0.1.0

.5   .5

.10

**WebVPN Client
172.26.26.1**

**Port forwarding security appliance parameters
(IP address):**
- **port-forward list—portlist**
- **WebVPN User Port—2222**
- **Remote Server—10.0.1.10**
- **Actual Port—23**
- **Example—**port-forward portlist 2222 10.0.1.10 23

**WebVPN parameters
(IP address):**
- **Need to launch port forwarding interface**
- **Telnet to "127.0.0.1 2222"**

WebVPN parameters (DNS):
- **Need to launch port forwarding interface**
- **Telnet to "Training"**

Port forwarding security appliance parameters (DNS):
- **port-forward list—portlist**
- **WebVPN User Port—2000**
- **Remote Server—Training**
- **Remote TCP Port—23**
- **Example—**port-forward portlist 2000 Training 23

SNPA v4.0—13-26

This example contrasts configuring port forwarding using DNS names versus using IP addresses. Keep the following in mind:

- If you use IP addresses, users need to have client applications point to a 127.0.0.1 address and local port that can vary from location to location when connecting over WebVPN. They must reconfigure applications to a real IP address and port when they connect locally.

- If you use hostnames, users can set their client applications to connect to the real hostname and TCP port for both remote WebVPN and directly connected sessions.

Define E-mail Proxy Servers

This topic covers how to configure the WebVPN e-mail proxy feature.

Enable E-mail Proxy for WebVPN Users
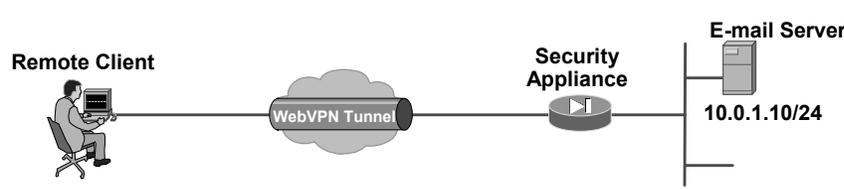

```
firewall(config-group-webvpn)#
```

```
functions {file-access | file-browsing | file-entry |
   filter | url-entry | mapi | port-forward | none}
```

- **Enables MAPI proxy for the group. Only necessary if using MAPI.**

```
fw1(config-group-webvpn)# functions mapi
```

SNPA v4.0—13-28

The **mapi** parameter enables or disables Microsoft Outlook/Exchange port forwarding at the group or user level and is only necessary if this feature is to be used.

Defining Proxy Servers

E-mail Server

Remote Client

Security Appliance

WebVPN Tunnel

10.0.1.10/24
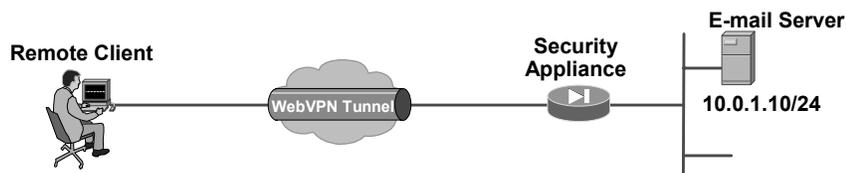
firewall(config)#

```
pop3s
smtps
imap4s
```

- **Enters the appropriate e-mail proxy subcommand mode**

```
fw1(config)# pop3s
fw1(config-pop3s)# ?
```

SNPA v4.0—13-29

Proxy servers are defined by entering the appropriate subcommand mode in global configuration mode. Proxy servers are available for POP3S, SMTPS, and IMAP4S. The following attributes can be configured in each subcommand mode:

- **port**—This specifies the port the POP3S proxy listens to. The default is 995. The value is limited to valid port numbers. Specifying **no port** reverts the value to the default.

- **authentication-server-group**—This specifies the set of authentication servers to use with POP3S. The default is to not have any authentication servers configured.

- **authorization-server-group**—This specifies the set of authorization servers to use with POP3S. The default is to not have any authorization servers configured.

- **accounting-server-group**—This specifies the set of accounting servers to use with POP3S. The default is to not have any accounting servers configured.

- **default-group-policy**—This specifies the name of the group policy that is to be used when AAA does not return a CLASSID attribute. If this command is not specified, and no CLASSID is specified, then the session is rejected. The **no** option removes this command from the configuration.

- **authentication**—This specifies the method of authentication that is required for POP3S connections. The user must always authenticate with the mailhost. The security appliance may optionally authenticate via a defined AAA server group (**aaa**), require an HTTPS WebVPN session to already be established (**piggyback**), and require certificate authentication (**certificate**). The default is to just authenticate to the mailhost. Specifying the command again overrides the previous setting. Specifying the **no** option reverts the value to the default by removing the command from the configuration.

- **server address**—This specifies the default POP3 server to be used when the user connects to the POP3S proxy and did not specify a POP3 server. The default is no server; thus an error would be returned back to the user if no POP3 server is specified by the client.

- **outstanding number**—This command specifies the number of outstanding, nonauthenticated sessions that are allowed. This is used to prevent denial of service (DoS) attacks by limiting the number of nonauthenticated sessions. When a new connection is made and the number of connections exceeds the given number, the oldest nonauthenticating connection is terminated; if there are no nonauthenticating connections, then the oldest authenticating connection is terminated. The default number is 20; the range is from 1 to 1000. The **no** option turns off this feature (in effect making the outstanding limit unlimited).

- **name-separator symbol**—This is the separator between the e-mail and VPN usernames and passwords. Choices are "@" (at), "|" (pipe), ":" (colon), "#" (hash), "," (comma), and ";" (semicolon). It must be different than the server separator. The default is ":". Specifying **no name-separator** removes the command from the configuration and reverts the value to the default.

- **server-separator symbol**—This is the separator between the e-mail and server names. Choices are "@" (at), "|" (pipe), ":" (colon), "#" (hash), "," (comma), and ";" (semicolon). It must be different than the name separator. The default is ":". Specifying **no server-separator** removes the command from the configuration and reverts the value to the default.

Defining E-Mail Server and Authentication Server

Cisco.com

E-mail Server

Remote Client

Security Appliance

WebVPN Tunnel
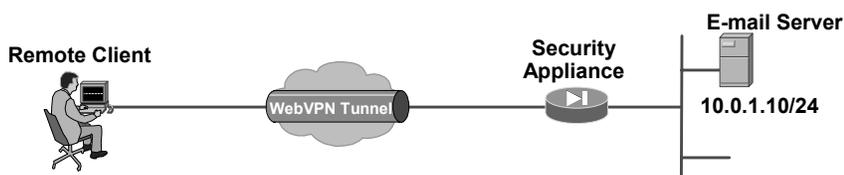
10.0.1.10/24

firewall(config-pop3s)#

```
server {ipaddr or hostname}
```

• **Specifies the default server for use with the e-mail proxy**

```
fw1(config-pop3s)# server 10.0.1.10
```

firewall(config-pop3s)#

```
authentication-server-group group tag
```

• **Specifies the authentication server to use with the e-mail proxy**

```
fw1(config-pop3s)# authentication-server-group AUTHSERVER
```

SNPA v4.0—13-30

Use the **server** command in the applicable e-mail proxy mode to specify a default e-mail proxy server. The security appliance sends requests to the default e-mail server when the user connects to the e-mail proxy without specifying a server. If you do not configure a default server and a user does not specify a server, the security appliance returns an error.

Use the **authentication-server-group** command to specify the previously configured authentication server or group of servers to use with the e-mail proxy.

Defining Authentication Type

Remote Client **Security Appliance** **E-mail Server**

WebVPN Tunnel

10.0.1.10/24
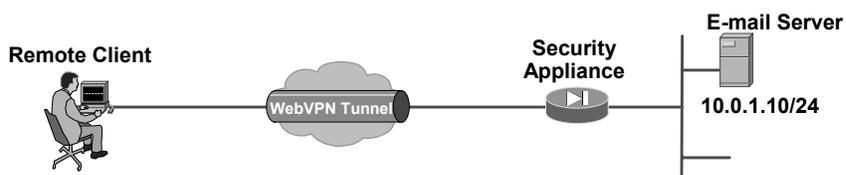
`firewall(config-pop3s)#`

```
authentication {aaa | certificate | mailhost | piggyback
```

- **Specifies the authentication method(s) that are used with the e-mail proxy**
- **Options are as follows:**
  - **aaa: Use previously configured AAA server for authentication**
  - **certificate: Use certificate for authentication**
  - **mailhost: Authenticates via the remote mail server (SMTPS only)**
  - **piggyback: Requires use of an established HTTPS WebVPN session**

```
fw1(config-pop3s)# authentication piggyback
```

SNPA v4.0—13-31

Use the **authentication** command to configure authentication methods for the e-mail proxy. To restore the default, AAA, use the **no** form of this command.

The syntax for the **authentication** command is as follows:

```
authentication {aaa | certificate | mailhost | piggyback}
```

aaa	Provides a username and password that the security appliance checks against a previously configured AAA server.
certificate	Provides a certificate during SSL negotiation.
mailhost	Authenticates via the remote mail server. You can configure mailhost for SMTPS only. For IMAP4S and POP3S, mailhost authentication is mandatory and not displayed as a configurable option.
piggyback	Requires that an HTTPS WebVPN session already exists.

Example: E-mail Proxy Configuration

Cisco.com

E-mail server

ASA

192.168.1.0   10.0.1.0

.5   .5   .10
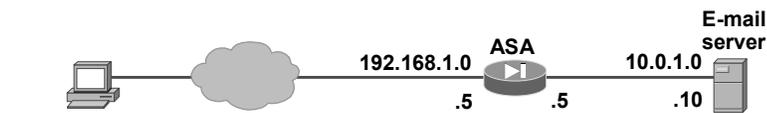
**WebVPN Client
172.26.26.1**

E-mail client parameters:
- Username—Student1
- Password—Student1
- POP address—192.168.1.5
- POP port—SSL port 995
- SMTP address (auth required)—192.168.1.5
- SMTP port—SSL port 988

Security appliance e-mail proxy parameters:
- POP3S ASA port—995
- POP3S default e-mail server—10.0.1.10
- POP3S auth. req.—e-mail server, piggyback HTTPS
- SMTPS default e-mail server—10.0.1.10
- SMTPS ASA port—988
- SMTPS auth. req.—piggyback HTTPS

E-mail server parameters:
- Username—Student1
- Password—Student1
- POP port—110
- SMTP port—25
- SMTP auth.—Required

SNPA v4.0—13-32

This example illustrates the various parameters that must be configured on each device. The main items of interest are the e-mail server address and port assignments entered on the e-mail client. These must match those configured on the security appliance, not those configured on the e-mail server. In this example, the username and password on the e-mail server and the security appliance are the same, so no special delimiters need to be used on the e-mail client.

Configure WebVPN Content Filters and ACLs

This topic covers how to configure the WebVPN content filters and ACL feature.

HTML Content Filtering

Cisco.com

Remote Client

Security Appliance

HTTP Server

WebVPN Tunnel

10.0.1.10/24

firewall(config)#

```
group-policy {name} attributes
```

• **Enters the group-policy attributes subcommand mode**

```
fw1(config)# group-policy WEBVPN1 attributes
```

firewall(config-group-policy)#

```
webvpn
```

• **Enters WebVPN group-policy attributes subcommand mode**

```
fw1(config-group-policy)# webvpn
```

SNPA v4.0—13-34

WebVPN content filters and ACLs are configured in the group-policy attributes webvpn subcommand mode.

HTML Content Filtering (Cont.)

HTTP Server

Remote Client

WebVPN Tunnel

Security Appliance

10.0.1.10/24
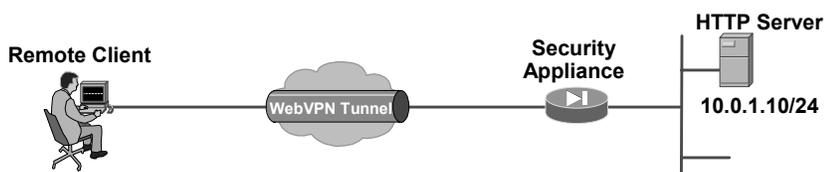
`firewall(config-group-webvpn)#`

```
html-content-filter {cookies | images | java | none | scripts}
```

- **Configures the content/objects to be filtered from the HTML for this policy**
- **Options are as follows:**
  - **cookies—Removes cookies from images, providing limited ad filtering and privacy**
  - **images—Removes references to images (removes <IMG> tags)**
  - **java—Removes references to Java and ActiveX (removes <EMBED>, <APPLET>, and <OBJECT> tags)**
  - **none—Indicates that there is no filtering; sets a null value, thereby disallowing filtering; prevents inheriting filtering values**
  - **scripts—Removes references to scripting (removes <SCRIPT> tags)**

```
fw1(config-group-webvpn)# html-content-filter cookies images java
```

SNPA v4.0—13-35

WebVPN content filtering lets you block or remove the parts of websites that use Java, ActiveX, and scripts, display images, and deliver cookies. By default, these parameters are disabled, which means that no filtering occurs.

WebVPN ACLs

Remote Client

Security Appliance

HTTP Server

WebVPN Tunnel

10.0.1.10/24
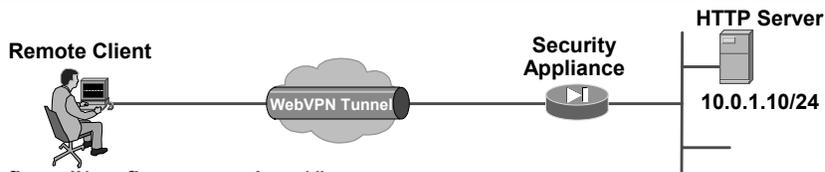
`firewall(config-group-webvpn)#`

```
filter {value ACLname | none}
```

- **Configures the name of the web-type ACL in the webvpn group-policy attributes submode**

```
fw1(config-group-webvpn)# filter value WEBVPNACL
```

`firewall(config)#`

```
access-list id webtype {deny | permit} url [url_string | any]
   [log [[disable | default] | level][interval secs] [time_range
   name]]
```

- **Configures a web-type ACL to be used for filtering with WebVPN**

```
fw1(config)# access-list WEBVPNACL webtype permit tcp any eq http
```

SNPA v4.0—13-36

You configure WebVPN ACLs to permit or deny various types of traffic for this user or group policy. These are filters that permit or deny user access to specific networks, subnets, hosts, and web servers.

Use the **filter** command in webvpn mode to specify the name of the ACL to use for WebVPN connections for this group policy or username. To remove the ACL, including a null value created by issuing the **filter none** command, use the **no** form of this command. The **no** option allows inheritance of a value from another group policy. To prevent inheriting filter values, use the **filter value none** command.

To add an ACL to the configuration that supports filtering for WebVPN, use the **access-list webtype** command in global configuration mode. Then use the **filter** command to apply those ACLs for WebVPN traffic.

Summary

This topic summarizes the information in this lesson.

Summary

- **WebVPN lets users establish a secure, remote-access VPN tunnel to a security appliance using a web browser.**
- **WebVPN features include:**
  - **Secure access to internal websites via HTTPS.**
  - **Windows Files Access, port forwarding, and e-mail proxy are supported.**
  - **HTML content filtering and WebVPN ACLs can be used to restrict WebVPN traffic.**

SNPA v4.0—13-37

Lesson 14

Configuring Transparent Firewall

Overview

This lesson provides an overview and explanation of transparent firewall mode. Enabling transparent firewall and monitoring and maintenance commands specific to the transparent firewall mode are also covered.

Objectives

Upon completing this lesson, you will be able to configure Cisco security appliances to run in transparent firewall mode. This ability includes being able to meet these objectives:

- Explain the purpose of transparent firewall mode

- Enable transparent firewall mode

- Monitor and maintain transparent firewall

Transparent Firewall Mode Overview

This topic provides an overview of the transparent firewall mode.

Transparent Versus Routed Firewall

Cisco.com

10.0.1.0
VLAN 100

VLAN 100
10.0.1.0

10.0.2.0
VLAN 100

VLAN 200
10.0.1.0

Routed Mode

Transparent Mode

The security appliance can run in two firewall settings:

- **Routed: Based on IP address**
- **Transparent: Based on MAC address**

SNPA v4.0—14-3
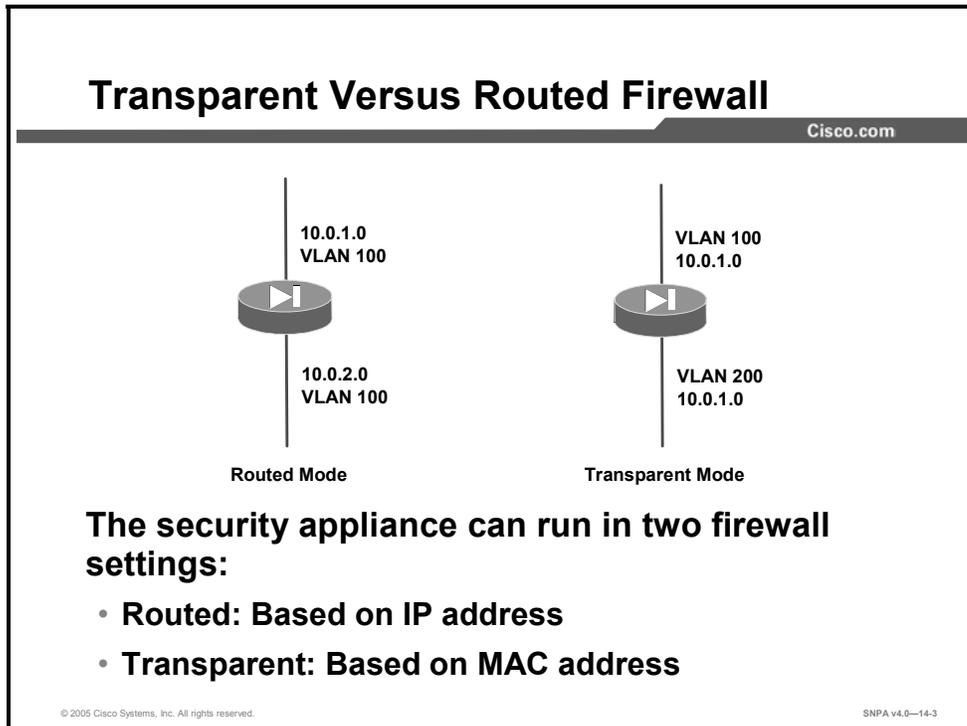
Traditionally, a firewall is a routed hop and acts as a default gateway for hosts that connect to one of its screened subnets. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a "bump in the wire" or a "stealth firewall" and is not seen as a router hop to connected devices. The security appliance connects the same network on its inside and outside ports, but each interface resides on a different VLAN.

- Transparent firewall mode only supports two interfaces, typically an inside interface and an outside interface.

- Transparent firewall mode can run in single as well as multiple context mode.

- The security appliance bridges packets from one VLAN to the other instead of routing them.

- MAC lookups are performed instead of routing table lookups.

Transparent Firewall Benefits

Easily integrated and maintained in existing network:

- **IP readdressing not necessary**
- **No NAT to configure**
- **No IP routing to troubleshoot**
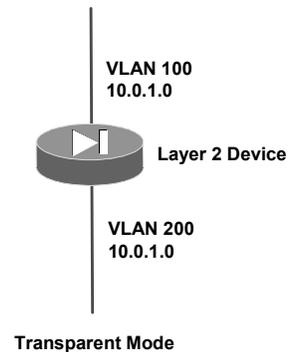
VLAN 100
10.0.1.0

Layer 2 Device

VLAN 200
10.0.1.0

Transparent Mode

Because the security appliance is not a routed hop, you can easily introduce a transparent firewall into an existing network; IP readdressing is unnecessary. Maintenance is facilitated because there are no complicated routing patterns to troubleshoot and no Network Address Translation (NAT) configuration.

Transparent Firewall Guidelines

- **Layer 3 traffic must be explicitly permitted.**
- **Each directly connected network must be on the same subnet.**
- **A management IP address is required for each context, even if you do not intend to use Telnet to the context.**
- **The management IP address must be on the same subnet as the connected network.**
- **Do not specify the security appliance management IP address as the default gateway for connected devices.**
  - **Devices need to specify the router on the other side of the security appliance as the default gateway.**
- **Each interface must be a different VLAN interface.**

Internet

10.0.1.10

VLAN 100
10.0.1.0

Transparent Mode   **Management IP Address 10.0.1.1**

VLAN 200
10.0.1.0

IP–10.0.1.3
Gateway – 10.0.1.10

IP–10.0.1.4
Gateway – 10.0.1.10
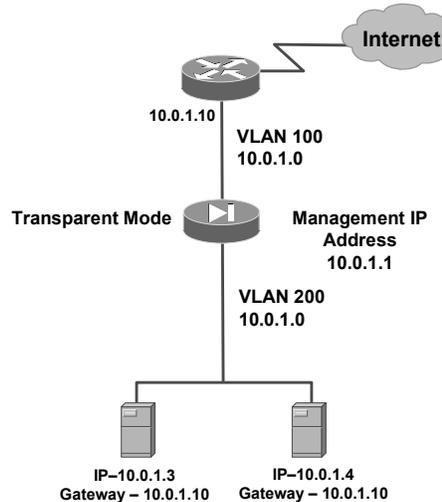
SNPA v4.0—14-5

Even though transparent mode acts as a bridge, Layer 3 traffic, such as IP traffic, cannot pass through the security appliance. The transparent firewall, however, can allow any traffic through using either an extended access control list (ACL) (for IP traffic) or an EtherType ACL (for non-IP traffic).The only traffic allowed through the transparent firewall without an ACL is Address Resolution Protocol (ARP) traffic. ARP traffic can be controlled by ARP inspection.

Note   The transparent mode security appliance does not pass Cisco Discovery Protocol (CDP) packets.

Because the security appliance is now acting as a bridge device, IP addressing should be configured as if the security appliance in not in the network. A management IP address is required for connectivity to and from the security appliance itself. The management IP address must be on the same subnet as the connected network. Keep in mind that as a Layer 2 device, the security appliance interfaces must be on different VLANs to differentiate the traffic flow.

Transparent Firewall Unsupported Features

The following features are not supported in transparent firewall mode:

- **NAT**
- **Dynamic routing protocols**
- **IPv6**
- **DHCP relay**
- **QoS**
- **Multicast**
- **VPN termination for through traffic**

VLAN 100
10.0.1.0

VLAN 200
10.0.1.0
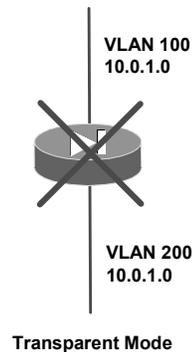
Transparent Mode

SNPA v4.0—14-6

The following features are not supported in transparent mode:

- NAT—NAT is performed on the upstream router.

- Dynamic routing protocols—You can, however, add static routes for traffic originating on the security appliance. You can also allow dynamic routing protocols through the security appliance using an extended ACL.

- IPv6

- Dynamic Host Configuration Protocol (DHCP) relay—The transparent firewall can act as a DHCP server, but it does not support the DHCP relay commands. DHCP relay is not required because you can allow DHCP traffic to pass through using an extended ACL.

- Quality of service (QoS)

- Multicast—You can, however, allow multicast traffic through the security appliance by allowing it in an extended ACL.

- VPN termination for through traffic—The transparent firewall supports site-to-site VPN tunnels for management connections only. It does not terminate VPN connections for traffic through the security appliance. You can pass VPN traffic through the security appliance using an extended ACL, but it does not terminate nonmanagement connections.

Enabling Transparent Firewall Mode

This topic explains how to enable transparent firewall mode.

Viewing the Current Firewall Mode

Cisco.com

10.0.1.0
VLAN 100

VLAN 100
10.0.1.0

?

10.0.2.0
VLAN 100

VLAN 200
10.0.1.0

Routed Mode

Transparent
Mode

firewall#

```
show firewall
```

• **Shows the current transparent firewall mode**

```
fw1# show firewall
Firewall mode: Transparent
```

SNPA v4.0—14-8

Use the **show firewall** command to view the current firewall mode. The mode will either be router or transparent.

Enabling Transparent Firewall Mode Versus Router Mode

```
10.0.1.0                        VLAN 100
VLAN 100                        10.0.1.0


10.0.2.0                        VLAN 200
VLAN 100                        10.0.1.0


Routed Mode                     Transparent
                                Mode
```
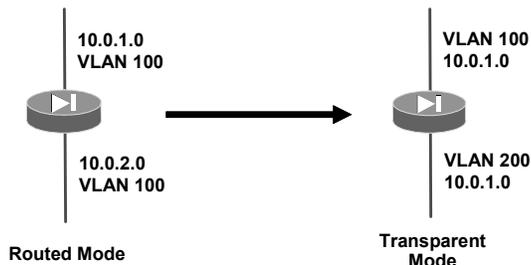
firewall(config)#

```
firewall transparent
```

• **Use the** no firewall transparent **command to return to router mode**

```
fw1(config)# firewall transparent
Switched to transparent mode
```

To set the firewall mode to transparent mode, use the **firewall transparent** command in global configuration mode. To restore routed mode, use the **no** form of this command.

For multiple context mode, you can use only one firewall mode for all contexts. You must set the mode in the system configuration. This command also appears in each context configuration for informational purposes only; you cannot enter this command in a context.

When you change modes, the security appliance clears the configuration because many commands are not supported for both modes.

Note	If you already have a populated configuration, be sure to back up your configuration before changing the mode; you can use this backup for reference when creating your new configuration.

If you download a text configuration to the security appliance that changes the mode with the firewall transparent command, be sure to put the command at the top of the configuration; the security appliance changes the mode as soon as it reads the command, then continues reading the configuration you downloaded. If the command is later in the configuration, the security appliance clears all the preceding lines in the configuration.

Assigning the Management IP Address

```
firewall#
```

```
ip address ip_address [mask] [standby ip_address]
```

- **Sets the IP address for an interface (in routed mode) or for the management address (transparent mode).**
- **For routed mode, enter this command in interface configuration mode.**
- **In transparent mode, enter this command in global configuration mode.**

```
fw1# ip address 10.0.1.1 255.255.255.0

fw1# show ip address

Management System IP Address:

        ip address 10.0.1.1 255.255.255.0

Management Current IP Address:

        ip address 10.0.1.1 255.255.255.0
```

A transparent firewall does not participate in IP routing. The only IP configuration required for the security appliance is to set the management IP address. This address is required because the security appliance uses this address as the source address for traffic originating on the security appliance, such as system messages and communications with AAA servers. You can also use this address for remote management access. This address must be on the same subnet as the upstream and downstream routers. For multiple context mode, set the management IP address within each context.

Configure ACLS

VLAN 100 **VLAN 200**
10.0.1.0 **10.0.1.0** **Internet**

10.0.1.11   10.0.1.2

firewall(config)#

```
access-list id [line line-number] [extended] {deny | permit}
{protocol | object-group protocol_obj_grp_id}{host sip | sip mask |
 interface ifc_name | object-group network_obj_grp_id | any}{host
 dip | dip mask | interface ifc_name | object-group
 network_obj_grp_id | any}[log [[level] [interval secs] | disable
 | default]][inactive | time-range time_range_name]
```

- **Determines which traffic should be allowed through the firewall.**
- **Remember that by default, no traffic is allowed through the firewall regardless of the security level that is assigned to the interfaces.**

```
fw1(config)# access-list ACLIN permit icmp 10.0.1.0 255.255.255.0
  10.0.1.0 255.255.255.0

fw1(config)# access-group ACLIN in interface inside

fw1(config)# access-group ACLIN in interface outside
```

SNPA v4.0—14-11

The transparent firewall can allow any traffic through using either an extended ACL (for IP traffic) or an EtherType ACL (for non-IP traffic). For example, you can establish routing protocol adjacencies through a transparent firewall; you can allow Open Shortest Path First (OSPF), Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP), or Border Gateway Protocol (BGP) traffic through based on an extended ACL. Likewise, protocols like Host Standby Routing Protocol (HSRP) or Virtual Router Redundancy Protocol (VRRP) can pass through the security appliance.

For features that are not directly supported on the transparent firewall, you can allow traffic to pass through so that upstream and downstream routers can support the functionality. For example, by using an extended ACL, you can allow DHCP traffic (instead of the unsupported DHCP relay feature) or multicast traffic such as that created by IP/TV.

EtherType ACLS
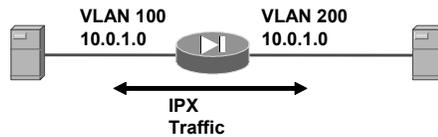
```
firewall(config)#
```

```
access-list id ethertype {deny | permit} {ipx | bpdu |
  mpls-unicast | mpls-multicast | any |hex_number}
```

Treatment of non-IP packets:

- **The transparent firewall introduces a new type of ACL: the EtherType ACL.**
- **With EtherType ACLs, an administrator can allow specific non-IP packets through the firewall.**

```
fw1(config)# access-list ETHER ethertype permit ipx
fw1(config)# access-group ETHER in interface inside
fw1(config)# access-group ETHER in interface outside
```

SNPA v4.0—14-12

To configure an ACL that controls traffic based on its EtherType, use the **access-list ethertype** command in global configuration mode.

Because EtherTypes are connectionless, you need to apply the ACL to both interfaces if you want traffic to pass in both directions.

The security appliance can control any EtherType that is identified by a 16-bit hexadecimal number. EtherType ACLs support Ethernet2 frames. 802.3-formatted frames are not handled by the ACL because they use a length field as opposed to a type field. Bridge protocol data units (BPDUs), which are handled by the ACL, are the only exception; they are Subnetwork Access Protocol (SNAP)-encapsulated, and the security appliance is designed to specifically handle BPDUs.

You can apply only one ACL of each type (extended and EtherType) to each direction of an interface. You can apply the same ACLs on multiple interfaces.

Predefined EtherTypes are:

- Internetwork Packet Exchange (IPX)

- BPDU

- MPLS

- Other Ethernet2 and DIX-encapsulated frames can be allowed based on their 2-byte EtherType.

- 802.3-encapsulated frames can't pass through the firewall at this time.

The syntax for the **access-list ethertype** command is as follows:

```
access-list id ethertype {deny | permit} {ipx | bpdu | mpls-
unicast | mpls-multicast | any | hex_number}
```

any	Specifies access to anyone.
bpdu	Specifies access to BPDUs. By default, BPDUs are denied.
deny	Denies access if the conditions are matched.
hex_number	A 16-bit hexadecimal number greater than or equal to 0x600 by which an EtherType can be identified.
Id	Name or number of an ACL.
ipx	Specifies access to IPX.
mpls-multicast	Specifies access to Multiprotocol Label Switching (MPLS) multicast.
mpls-unicast	Specifies access to MPLS unicast.
permit	Permits access if the conditions are matched.

firewall(config)#

```
arp interface_name ip_address mac_address [alias]
```

- **A static ARP entry maps an MAC address to an IP address and identifies the interface through which the host is reached.**

```
fw1(config)# arp outside 10.0.1.1 0009.7cbe.2100
```

firewall(config)#

```
arp-inspection interface_name enable [flood | no-flood]
```

- **ARP inspection checks all ARP packets against static ARP entries and blocks mismatched packets.**
- **This feature prevents ARP spoofing.**

```
fw1(config)# arp-inspection outside enable

arp inspection enabled on outside
```

SNPA v4.0—14-13

ARP inspection prevents malicious users from impersonating other hosts or routers (known as ARP spoofing). ARP spoofing can enable a "man-in-the-middle" attack. For example, a host sends an ARP request to the gateway router; the gateway router responds with the gateway router MAC address. The attacker, however, sends another ARP response to the host with the attacker MAC address instead of the router MAC address. The attacker can now intercept all the host traffic before forwarding it on to the router. ARP inspection ensures that an attacker cannot send an ARP response with the attacker MAC address, so long as the correct MAC address and the associated IP address are in the static ARP table.

Configure static ARP entries using the **arp** command before you enable ARP inspection.

When you enable ARP inspection, the security appliance compares the MAC address, IP address, and source interface in all ARP packets to static entries in the ARP table, and takes the following actions:

- If the IP address, MAC address, and source interface match an ARP entry, the packet is passed through.

- If there is a mismatch between the MAC address, the IP address, or the interface, then the security appliance drops the packet.

- If the ARP packet does not match any entries in the static ARP table, then you can set the security appliance to either forward the packet out all interfaces (flood), or to drop the packet.

Note   The management-specific interface, if present, never floods packets even if this parameter is set to flood.

The syntax for the **arp-inspection** command is as follows:

```
arp-inspection interface_name enable [flood | no-flood]
```

enable	Enables ARP inspection.
flood	(Default) Specifies that packets that do not match any element of a static ARP entry are flooded out all interfaces except the originating interface. If there is a mismatch between the MAC address, the IP address, or the interface, then the security appliance drops the packet. Note: The management-specific interface, if present, never floods packets even if this parameter is set to flood.
interface_name	The interface on which you want to enable ARP inspection.
no-flood	(Optional) Specifies that packets that do not exactly match a static ARP entry are dropped.

Monitoring and Maintaining Transparent Firewall Mode

This topic covers monitoring and maintenance commands specific to transparent firewall mode.

MAC Address Table

Cisco.com

VLAN 100
10.0.1.0

VLAN 200
10.0.1.0

0010.7cbe.6101

```
Interface MAC Address Type Time Left
------------------------------------------------
outside 0009.7cbe.2100 dynamic 10 -
inside 0010.7cbe.6101 dynamic 10 -
```

0009.7cbe.2100

The MAC address table is used to find the outgoing interface based on the destination MAC address.

- **Built on the fly; contents learned from source MAC addresses**
- **No flooding if MAC address not found**

SNPA v4.0—14-15

The security appliance learns and builds a MAC address table in a way that is similar to a normal bridge or switch: When a device sends a packet through the security appliance, the security appliance adds the MAC address to its table. The table associates the MAC address with the source interface so that the security appliance knows to send any packets addressed to the device out the correct interface.

Because the security appliance is a firewall, if the destination MAC address of a packet is not in the table, the security appliance does not flood the original packet on all interfaces as a normal bridge does. Instead, it generates the following:

■ Packets for directly connected devices—The security appliance generates an ARP request for the destination IP address, so that the security appliance can learn which interface receives the ARP response.

■ Packets for remote devices—The security appliance generates a ping to the destination IP address so that the security appliance can learn which interface receives the ping reply.

The original packet is dropped.

Disabling MAC Address Learning

VLAN 100
10.0.1.0

VLAN 200
10.0.1.0

0010.7cbe.6101

Interface MAC Address Type Time Left
----
outside 0009.7cbe.2100 dynamic 10 -
inside 0010.7cbe.6101 dynamic 10 -

0009.7cbe.2100
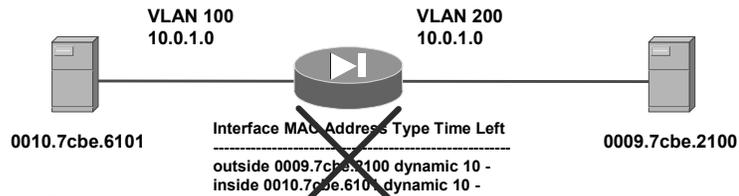
firewall(config)#

```
mac-learn interface_name disable
no mac-learn interface_name disable
```

- **Disables MAC address learning for an interface.**
- **To reenable MAC address learning, use the** no **form of this command.**
- **By default, each interface automatically learns the MAC addresses of entering traffic, and the security appliance adds corresponding entries to the MAC address table.**

```
fw1(config)# mac-learn outside disable

Disabling learning on outside
```

SNPA v4.0—14-16

By default, each interface automatically learns the MAC addresses of entering traffic, and the security appliance adds corresponding entries to the MAC address table. You can disable MAC address learning if desired; however unless you statically add MAC addresses to the table, no traffic can pass through the security appliance.

Adding a Static MAC Address

VLAN 100
10.0.1.0

VLAN 200
10.0.1.0

0010.7cbe.6101

Interface MAC Address Type Time Left
----
outside 0009.7cbe.2100 static -
inside 0010.7cbe.6101 static -

0009.7cbe.2100
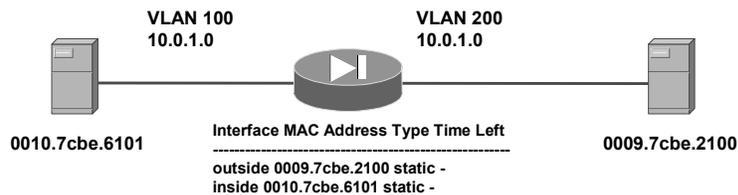
firewall(config)#

```
mac-address-table static interface_name mac_address
```

- **Adds a static entry to the MAC address table.**
- **Normally, MAC addresses are added to the MAC address table dynamically as traffic from a particular MAC address enters an interface.**
- **Guard against MAC spoofing.**

```
fw1(config)# mac-address-table static inside 0010.7cbe.6101
Added <0010.7cbe.6101> to the bridge table
```

SNPA v4.0—14-17

Normally, MAC addresses are added to the MAC address table dynamically as traffic from a particular MAC address enters an interface. You can add static MAC addresses to the MAC address table if desired. One benefit to adding static entries is to guard against MAC spoofing. If a client with the same MAC address as a static entry attempts to send traffic to an interface that does not match the static entry, then the security appliance drops the traffic and generates a system message.

Viewing the MAC Address Table

firewall#

```
show mac-address-table [interface_name | count | static]
```

- **Shows the MAC address table.**

```
fw1# show mac-address-table

interface mac  address          type      Age(min)

-------------------------------------------------------------

inside  0010.7cbe.6101          static

inside  0008.e3bc.5ee0          dynamic   5
```

SNPA v4.0—14-18

You can view the entire MAC address table (including static and dynamic entries for both interfaces), or you can view the MAC address table for an interface.

debug Commands

Debug Support

- debug arp-inspection**: To track code path of ARP forwarding and ARP inspection module in transparent firewall**
- debug mac-address-table**: To track insert/delete/update to the bridge table maintained for transparent firewall**

```
fw1# debug arp-inspection
fw1# debug mac-address-table
```

SNPA v4.0—14-19

Two new **debug** commands have been introduced with regard to transparent firewall mode:

- **debug arp-inspection**—Shows debug messages for ARP inspection
- **debug mac-address-table**—Shows debug messages for the MAC address table

Summary

This topic summarizes the information you learned in this lesson.

Summary

- A transparent firewall is a Layer 2 firewall that acts like a "bump in the wire or a "stealth firewall" and is not seen as a router hop to connected devices.

- The PIX Firewall connects the same network on its inside and outside ports but uses different VLANs on the inside and outside.

- By default, no traffic is allowed through the firewall regardless of the security level assigned to the interfaces. ACLs must be defined.

- Layer 2 monitoring and maintenance is performed by customizing the MAC address table.

SNPA v4.0—14-20

Lesson 15

Configuring Security Contexts

Overview

This lesson describes the purpose of security contexts and how to enable, configure, and manage multiple contexts.

Objectives

Upon completing this lesson, you will be able to configure the security appliance to support multiple contexts. This ability includes being able to meet these objectives:

- Explain the purpose of security contexts
- Enable and disable multiple context mode
- Configure a security context
- Manage a security context

Security Context Overview

This topic provides an overview of security contexts.

Virtualization

Cisco.com

- **You can partition a single security appliance into multiple virtual firewalls, known as security contexts.**
- **Each context has its own configuration that identifies the security policy, interfaces, and almost all the options you can configure on a stand-alone firewall.**
- **The system administrator adds and manages contexts by configuring them in the system configuration, which identifies basic settings for the security appliance.**
- **When the system needs to access network resources, it uses one of the contexts that is designated as the admin context.**

Security Appliance
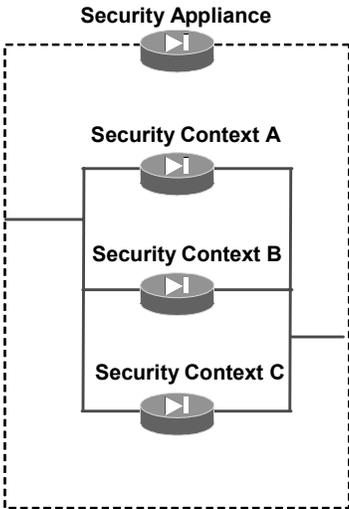
Security Context A

Security Context B

Security Context C

SNPA v4.0—15-3

You can partition a single security appliance into multiple virtual firewalls, known as security contexts. Each context is an independent firewall, with its own security policy, interfaces, and administrators. Having multiple contexts is similar to having multiple stand-alone firewalls.

Each context has its own configuration that identifies the security policy, interfaces, and almost all the options you can configure on a stand-alone firewall. If desired, you can allow individual context administrators to implement the security policy on the context. Some resources are controlled by the overall system administrator, such as VLANs and system resources, so that one context cannot affect other contexts inadvertently.

The system administrator adds and manages contexts by configuring them in the system configuration, which identifies basic settings for the security appliance. The system administrator has privileges to manage all contexts. The system configuration does not include any network interfaces or network settings for itself; rather, when the system needs to access network resources (such as downloading the contexts from the server), it uses one of the contexts that is designated as the admin context.

The admin context is just like any other context, except that when a user logs into the admin context, that user has system administrator rights and can access the system execution space and all other contexts. Typically, the admin context provides network access to network-wide resources, such as a syslog server or context configuration server.

Common Uses for Security Contexts

Multiple security contexts can be used in the following situations:

- **Service provider wanting to sell firewall services to many customers**
- **Large enterprise or a college campus wanting to keep departments completely separate**
- **Enterprise wanting to provide distinct security policies to different departments**
- **Any network requiring more than one firewall**

Security Appliance

Security Context A — Company A

Security Context B — Company B
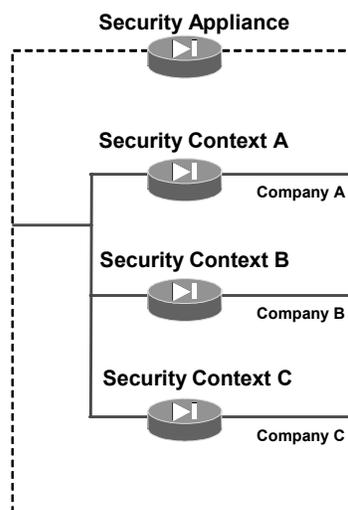
Security Context C — Company C

SNPA v4.0—15-4

You might want to use multiple security contexts in the following situations:

- You are a service provider and want to sell firewall services to many customers.

- You are a large enterprise or a college campus and want to keep departments completely separate.

- You are an enterprise that wants to provide distinct security policies to different departments.

- You have a network that requires more than one firewall.

Service Provider-Managed Security Appliance with Multiple Contexts

Service Provider   Customer Prem

Internet

VFW1

VFW2

VFW3

VFW4

- **Same service as available with multiple security appliances**
- **Now available in smaller, more manageable package**
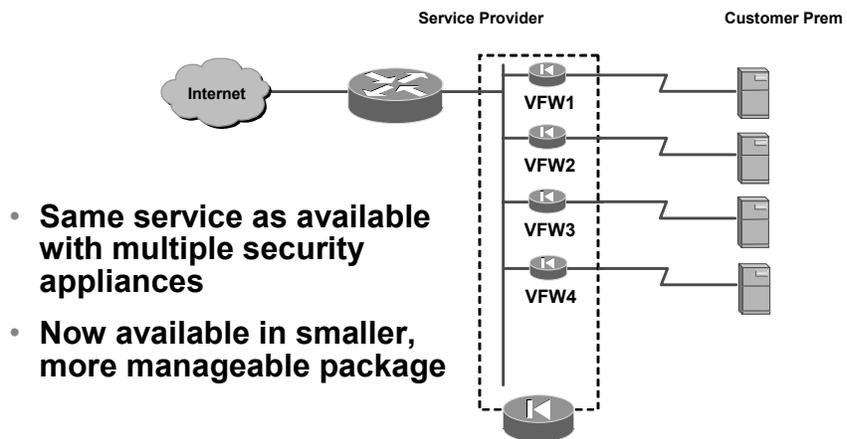
SNPA v4.0—15-5

In this example, a service provider is using a single security appliance divided into multiple contexts to deliver the same service as multiple stand-alone small security appliances. By enabling multiple security contexts on the security appliance, the service provider can implement a cost-effective, space-saving solution that keeps all customer traffic separate and secure, and also eases configuration.

Context Configuration Files

Context configuration files have the following characteristics:

- **Each context has its own configuration file.**

- **The security appliance also includes a system configuration that identifies basic settings for the security appliance, including a list of contexts.**

Security Appliance

System Config

Security Context Admin

Security Context Admin Config

Security Context B

Security Context B Config
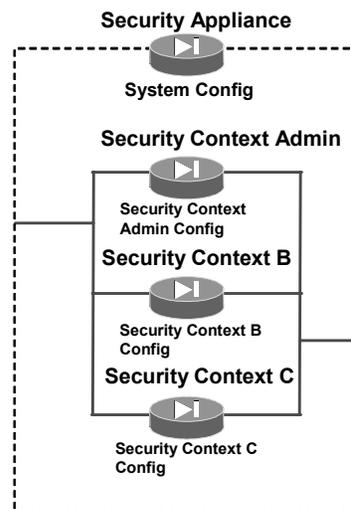
Security Context C

Security Context C Config

SNPA v4.0—15-6

Each context has its own configuration file that identifies the security policy, interfaces, and almost all the options you can configure on a stand-alone firewall. You can store context configurations on the local disk partition on the Flash memory card, or you can download them from a TFTP, FTP, or Hypertext Transfer Protocol secure (HTTPS) server.

In addition to system configurations in individual security contexts, the security appliance also includes a system configuration that identifies basic settings for the security appliance, including a list of contexts. Like the single-mode configuration, the security appliance configuration resides as the startup configuration in the Flash memory partition.

Packet Classification

Security Appliance

Each packet that enters the security appliance must be classified, so that the security appliance can determine to which context to send a packet. The security appliance checks for the following characteristics:

- **Source interface (VLAN)**
- **Destination address**

The security appliance uses the characteristic that is unique and not shared across contexts.

- **You can share a VLAN interface as long as each IP address space on that VLAN is unique.**
- **You can have overlapping IP addresses as long as the VLANs are unique.**

Security Context A — vlan1 — 192.168.0.1

Security Context B — vlan2 — 192.168.0.1

Security Context C — vlan3 — 192.168.0.1
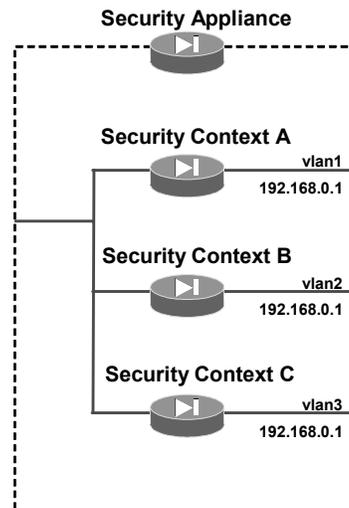
SNPA v4.0—15-7

Each packet that enters the security appliance must be classified so that the security appliance can determine to which context to send a packet. The security appliance checks for the following characteristics:

- Source interface (VLAN)
- Destination address

In classifying the packets, the security appliance uses the characteristic of each packet that is unique and not shared across contexts. For example, if you share a VLAN across contexts, the classifier uses the IP address. You can share a VLAN interface as long as each IP address space on that VLAN is unique, or you can have overlapping IP addresses as long as the VLANs are unique. The figure shows multiple contexts sharing an outside VLAN, while the inside VLANs are unique, allowing overlapping IP addresses.

Enabling Multiple Context Mode

This topic describes how to enable multiple contexts on the security appliance.

Backing Up the Single-Mode Configuration

Cisco.com

When you convert from single mode to multiple mode, the running configuration is converted into two files:

- **New startup configuration that comprises the system configuration**
- **Admin.cfg that comprises the admin context**

The original running configuration is saved as old_running.cfg (in disk).

Security Appliance Multimode

System Config

Security Appliance Single Mode

Security Context Admin

Running Config

Admin Config

old_running.cfg Config

SNPA v4.0—15-9

When you convert from single mode to multiple mode, the security appliance converts the running configuration into two files: a new startup configuration (in Flash memory) that comprises the system configuration, and admin.cfg (in the disk partition) that comprises the admin context. The original running configuration is saved as old_running.cfg (in disk). The original startup configuration is not saved, therefore if it differs from the running configuration, you should back it up before proceeding.

The Admin Context

The admin context has the following characteristics:

- **The system execution space has no traffic-passing interfaces, and uses the policies and interfaces of the admin context to communicate with other devices.**
- **Used to fetch configs for other contexts and send system-level syslogs.**
- **Users logged in to the admin context are able to change to the system context and create new contexts.**
- **Aside from its significance to the system, it could be used as a regular context.**

Security Appliance Multimode

System Config

Security Context Admin

Admin Config

Security Context A   Security Context B
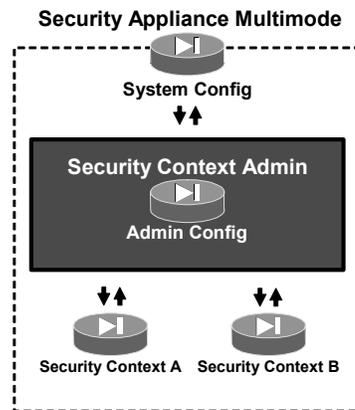
SNPA v4.0—15-10

The system configuration does not include any network interfaces or network settings for itself; instead, when the system needs to access network resources (such as downloading the contexts from a server), it uses one of the contexts that is designated as the admin context. If your system is already in multiple context mode, or if you convert from single mode, the admin context is created automatically as a file on the disk partition called admin.cfg.

The admin context has the following characteristics:

- The system execution space has no traffic-passing interfaces, and uses the policies and interfaces of the admin context to communicate with other devices.
- The admin context is used to fetch configs for other contexts and send system-level syslogs.
- Users logged in to the admin context are able to change to the system context and create new contexts.
- Aside from its significance to the system, it could be used as a regular context.

Viewing the Current Context Mode

firewall#

```
show mode
```

• **Shows the current firewall mode.**

```
fw1# show mode
Firewall mode: multiple
The flash mode is the SAME as the running mode.
```

SNPA v4.0—15-11

Use the **show mode** command in privileged EXEC mode to show the security context mode for the running software image and for any image in Flash memory. The firewall mode will be one of these types of modes:

■ **single mode:** Multiple mode disabled

■ **multiple mode:** Multiple mode enabled

Enabling and Disabling Multiple Context Mode

firewall#

```
mode {single | multiple} [noconfirm]
```

Selects the context mode as follows:

- **`multiple`: Sets multiple context mode; mode with security contexts**
- **`single`: Sets single context mode; mode without security contexts**
- **`noconfirm`: Sets the mode without prompting you for confirmation.**

Before you convert from multiple mode to single mode, you might want to copy the backup version of the original running configuration to the current startup configuration.

```
fw1# mode multiple
```

SNPA v4.0—15-12

To set the security context mode to single or multiple, use the **mode** command in global configuration mode. In single mode, the security appliance has a single configuration and behaves as a single device. In multiple mode, you can create multiple contexts, each with its own configuration. The number of contexts allowed depends on your license.

If you convert from multiple mode to single mode, you might want to first copy a full startup configuration (if available) to the security appliance; the system configuration inherited from multiple mode is not a complete functioning configuration for a single-mode device.

Configuring a Security Context

This topic describes how to configure a security context.

Adding a Context

firewall(config)#

```
context name
```

Adds or modifies a context.

- **Name**: **A string up to 32 characters long (case-sensitive).**
- **"System" or "Null" (in uppercase or lowercase letters) are reserved names, and cannot be used.**

```
fw1(config)# context context1
Creating context 'context1'... Done. (4)
fw1(config-ctx)#
```

SNPA v4.0—15-14

Use the **context** command in global configuration mode to create a security context in the system configuration and enter context configuration mode. The security context definition in the system configuration identifies the context name, configuration file URL, VLAN, and interfaces that a context can use.

If you do not have an admin context (for example, if you clear the configuration), the first context you add must be the admin context. After you specify the admin context, you can enter the **context** command to configure the admin context.

Config Context Submode: Allocating Interfaces

```
firewall(config-ctx)#
```

```
allocate-interface physical_interface.subinterface[-
  physical_interface.subinterface][map_name[-
  map_name]][visible | invisible]
```

- **Interfaces must initially be enabled in system configuration mode before being allocated to a context.**
- **Initially the context created will not have access to any interfaces.**
- **Interfaces must be added using the** allocate-interface **command.**

```
fw1(config-ctx)# allocate-interface gigabitethernet0/1
fw1(config-ctx)# allocate-interface gigabitethernet1/1.100 int1
```

SNPA v4.0—15-15

To allocate interfaces to a security context, use the **allocate-interface** command in system configuration mode.

You can enter this command multiple times to specify different ranges. In transparent firewall mode, you can only use two interfaces per context. If your security appliance model includes a management interface, you can configure that interface for management traffic in addition to two network interfaces. You can assign the same interfaces to multiple contexts in routed mode, if desired. Transparent mode does not allow shared interfaces.

If you specify a range of subinterfaces, you can specify a matching range of mapped names. Follow these guidelines for ranges:

- The mapped name must consist of an alphabetic portion followed by a numeric portion. The alphabetic portion of the mapped name must match for both ends of the range. For example, enter the following range: int0-int10.

- The numeric portion of the mapped name must include the same quantity of numbers as the subinterface range. For example, if both ranges include 100 interfaces, enter the following range: gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int100

The syntax for the **allocate-interface** command is as follows:

```
allocate-interface physical_interface [map_name] [visible |
invisible]
allocate-interface physical_interface.subinterface[-
physical_interface.subinterface] [map_name[-map_name]]
[visible | invisible]
```

invisible	(Default) Allows context users to only see the mapped name (if configured) in the output from the **show interface** command.
map_name	(Optional) Sets a mapped name. The *map_name* is an alphanumeric alias for the interface that can be used within the context instead of the interface ID. If you do not specify a mapped name, the interface ID is used within the context. For security purposes, you might not want the context administrator to know which interfaces are being used by the context. A mapped name must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, or an underscore. For example, you can use the following names: • **int0** • **inta** • **int_0** For subinterfaces, you can specify a range of mapped names.
physical_interface	Sets the interface ID.
subinterface	Sets the subinterface number. You can identify a range of subinterfaces.
visible	(Optional) Allows context users to see physical interface properties in the output from the **show interface** command, even if you set a mapped name.

Configuration of Contexts

Each context has its own configuration file, which is specified using the config-url **command.**

Until the config-url **command has been entered, the context is not operational.**

The config-url **command accepts the following URL types:**

- **disk0/flash: Configurations stored on the Flash filesystem of the device**
- **disk1: Configurations stored on the compact Flash memory card of the device**
- **tftp: TFTP server-based configurations**
- **ftp: FTP server-based configurations**
- **https: Webserver-based configurations (read-only)**

SNPA v4.0—15-16

Each context on the security appliance has its own configuration file which is specified using the **config-url** command. Until you enter the **config-url** command, the context is not operational. The context becomes operational when you enter the **config-url** command.

The configuration files can be stored in a variety of locations. Note that HTTPS locations are read-only. Also, all remote URLs must be accessible from the admin context.

Note	Enter the **allocate-interface** command(s) before you enter the **config-url** command. The security appliance must assign interfaces to the context before it loads the context configuration; the context configuration might include commands that refer to interfaces (such as **interface**, **nat**, **global**). If you enter the **config-url** command first, the security appliance loads the context configuration immediately. If the context contains any commands that refer to interfaces, those commands fail.

Config Context Submode: Designating the Configuration File

firewall(config-ctx)#

```
config-url url
```

- **Identifies the URL from which the system downloads the context configuration.**
- **When you add a context URL, the system immediately loads the context so that it is running.**
- **If the system cannot retrieve the context configuration file, the system creates a blank context.**
- **Also used to change the URL of a previously configured context.**

```
fw1(config-ctx)# config-url disk0:/context3.cfg
fw1(config-ctx)# show run
…
context context3
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/1
  config-url disk0:/context3.cfg
…
```

SNPA v4.0—15-17

To identify the URL from which the system downloads the context configuration, use the **config-url** command in context configuration mode. Note the following:

- When you add a context URL, the system immediately loads the context so that it is running.

- The admin context file must be stored on the Flash memory DIMM.

- If the system cannot retrieve the context configuration file because the server is unavailable, or the file does not yet exist, the system creates a blank context that is ready for you to configure with the command-line interface.

- To change the URL, reenter the **config-url** command with a new URL.

    — The security appliance merges the new configuration with the current running configuration. Reentering the same URL also merges the saved configuration with the running configuration. A merge adds any new commands from the new configuration to the running configuration. If the configurations are the same, no changes occur. If commands conflict or if commands affect the running of the context, then the effect of the merge depends on the command. You might get errors, or you might have unexpected results. If the running configuration is blank (for example, if the server was unavailable and the configuration was never downloaded), then the new configuration is used.

    — If you do not want to merge the configurations, you can clear the running configuration, which disrupts any communications through the context, and then reload the configuration from the new URL.

The syntax for the **config-url** command is as follows:

```
config-url url
```

url	Sets the context configuration URL. All remote URLs must be accessible from the admin context, with the following URL syntax:
	■ **disk0:/**[*path/*]*filename*—This option is only available for the ASA platform, and indicates the Flash memory DIMM. You can also use **flash** instead of **disk0**; they are aliased.
	■ **disk1:/**[*path/*]*filename*—This option is only available for the ASA platform, and indicates the compact Flash memory card.
	■ **flash:/**[*path/*]*filename*—This option indicates the Flash memory DIMM.
	■ **ftp:**//[*user*[*:password*]*@*]*server*[*:port*]/[*path/*]*filename*[**;type=***xx*]
	■ The **type** can be one of the following keywords:
	— **ap**—ASCII passive mode
	— **an**—ASCII normal mode
	— **ip**—(Default) Binary passive mode
	— **in**—Binary normal mode
	■ **http**[**s**]**://**[*user*[*:password*]*@*]*server*[*:port*]/[*path/*]*filename*
	■ **tftp://**[*user*[*:password*]*@*]*server*[*:port*]/[*path/*]*filename*[**;int=***interface_name*]
	Specify the interface name if you want to override the route to the server address.

Saving Context Configurations

After the context has been activated, it is configured much the same as any security appliance stand-alone device, as follows:

- **Once in a context, you can enter the configuration mode to modify the context configuration.**
- **The startup configuration for a context resides where the** config-url **command specifies.**
- **The location of the startup configuration cannot be changed from within the context.**
- Write mem**,** copy run start**, etc., all manipulate the configuration location specified by the** config-url **command.**

The running configuration that you edit in configuration mode, or that is used in the **copy** or **write** commands, depends on your location. When you are in the system execution space, the running configuration consists only of the system configuration; when you are in a context, the running configuration consists only of that context.

After the context has been activated, it is configured much the same as any security appliance stand-alone device. Individual device configuration changes made in the context are stored in the configuration file specified by the **config-url** command. The location of the startup configuration file cannot be changed or viewed from within the context.

Managing Security Contexts

This section describes how security contexts are managed.

Removing a Security Context

firewall(config)#

```
no context name
```

- **You can only remove a context by editing the system configuration.**
- **You cannot remove the current admin context, unless you remove all contexts.**
- **Contexts can be removed or created on the fly; no reboot is required.**

```
fw1(config)# no context context3
WARNING: Removing context 'context3'
Proceed with removing the context? [confirm]
```

firewall(config)#

```
clear configure context
```

- **Removes all contexts, including the admin context**

SNPA v4.0—15-20

You can only remove a context by editing the system configuration. To remove a context, use the **no** form of the **context** command. You cannot remove the current admin context, unless you remove all contexts. To clear all context configurations in the system configuration, use the **clear configure context** command in global configuration mode. Context can be created or removed without a reboot.

Note   If you use failover, there is a delay between when you remove the context on the active unit and when the context is removed on the standby unit. You might see an error message indicating that the number of interfaces on the active and standby units are not consistent; this error is temporary and you can ignore it.

Changing the Admin Context

firewall(config)#

```
admin-context name
```

- **You can set any context to be the admin context.**

```
fw1(config)# admin-context context2
fw1(config)# show run
…
admin-context context2
context context2
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/3
  config-url disk0:/context2.cfg
…
```

SNPA v4.0—15-21

Use the **admin-context** command in global configuration mode to set the admin context for the system configuration. You can set any context to be the admin context, as long as the context configuration resides on the internal Flash memory.

Changing Between Contexts

firewall(config)#

```
changeto {system | context name}
```

- **Changes the environment to the context specified.**

```
fw1(config)# changeto context context1
fw1/context1(config)#
```

- **Also changes the environment to the system execution space.**

```
fw1/context1(config)# changeto context system
fw1(config)#
```

SNPA v4.0—15-22

If you log into the system execution space or the admin context, you can change between contexts and perform configuration and monitoring tasks within each context. Use the **changeto** command in privileged EXEC mode to change between security contexts and the system context.

Viewing Context Information

```
firewall(config)#
```

```
show context [name [detail]| count]
```

- **View all contexts.**
- **An "*" designates an admin context.**

```
fw1(config)# show context
Context Name     Interfaces                     URL
*admin           GigabitEthernet0/0,GigabitEthernet0/1 disk0:/admin.cfg
 context1        GigabitEthernet0/0,GigabitEthernet0/1,GigabitEthernet0/3 disk0
:/context1.cfg
 context2        GigabitEthernet0/0,GigabitEthernet0/1,GigabitEthernet0/3 disk0
:/context2.cfg
Total active Security Contexts: 3…
```

Use the **show context** command to view all contexts. From the system execution space, you can view a list of contexts including the name, interfaces, and configuration file. In the system execution space, the security appliance displays all contexts if you do not specify a name.

Viewing Context Information (Cont.)

firewall(config)#

```
show context [name [detail]| count]
```

- **The** detail **option shows additional information.**
- **The** count **option shows the total number of contexts.**

```
fw1(config)# sh context detail
Context "admin", has been created, but initial ACL rules not complete
  Config URL: disk0:/admin.cfg
  Real Interfaces: GigabitEthernet0/0, GigabitEthernet0/1
  Mapped Interfaces: GigabitEthernet0/0, GigabitEthernet0/1
  Flags: 0x00000013, ID: 1
…
```

SNPA v4.0—15-24

The **show context detail** command reveals additional details about the context(s), including the running state and information for internal use.

The **show context count** command lists the number of contexts configured.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

- **Virtual firewalls allow you to separate the security appliance into multiple independent firewalls called security contexts.**
- **Packets can be classified by VLAN or address.**
- **Security contexts can be managed and configured independently.**

SNPA v4.0—15-25

Lesson 16

Failover

Overview

This lesson describes security appliance failover options and how to configure them. The lesson describes the types of failover supported by the security appliance, and how to configure active/standby, active/active, and stateful failover.

Objectives

Upon completing this lesson, you will be able to implement and configure failover in a network. This ability includes being able to meet these objectives:

- Describe the difference between hardware and stateful failover
- Describe the difference between active/standby and active/active failover
- Define the security appliance failover hardware requirements
- Describe how active/standby failover works
- Explain the security appliance roles of primary, secondary, active, and standby
- Describe how active/active failover works
- Configure active/standby cable-based and LAN-based failover
- Configure active/active failover

Understanding Failover

This topic describes failover—what it is and how it works.

Failover enables the standby security appliance to take over the duties of the active security appliance when the active security appliance fails. The following are the two categories of failover:

- Hardware failover: Hardware failover provides hardware redundancy. When the active security appliance fails, the standby security appliance becomes active. All connections are lost, and client applications must perform a new connection to restart communication through the security appliance. The disconnection happens because the active security appliance does not pass the stateful connection information to the standby security appliance. Failover messages are exchanged over a serial failover cable or a LAN-based failover connection.

- Stateful failover: The stateful failover feature passes per-connection stateful information to the standby unit. After a failover occurs, the same connection information is available at the new active unit. Most end-user applications are not required to do a reconnect to keep the same communication session. The state information passed to the standby unit includes information such as the global pool addresses and status; connection and translation information and status; the negotiated H.323, Session Initiation Protocol (SIP), and Media Gateway Control Protocol (MGCP) User Datagram Protocol (UDP) ports; the port allocation map for port address translation (PAT); and other details necessary to let the standby unit take over processing if the primary unit fails.

Hardware Failover: Active/Standby
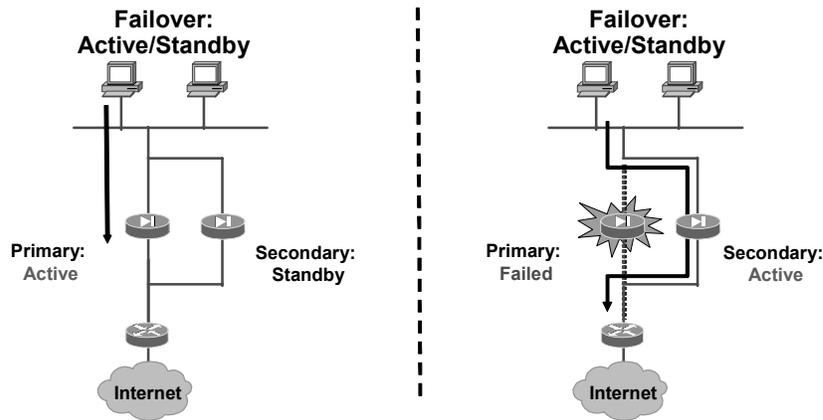
The hardware failover function for the security appliance provides a safeguard in case a security appliance fails. Specifically, when one security appliance fails, another immediately takes its place. In the failover process, there are two security appliances: the primary security appliance and the secondary security appliance. The primary security appliance functions as the active security appliance, performing normal network functions. The secondary security appliance functions as the standby security appliance, ready to take control should the active security appliance fail to perform. When the primary security appliance fails, the secondary security appliance becomes active while the primary security appliance enters the failed state. This entire process is called failover.

There are two types of hardware failover: active/standby and active/active. In active/standby, one security appliance is actively processing traffic while the other is a hot standby. All traffic flows through the active security appliance. In the example in the figure, the active/standby scenario consists of two security appliances, the primary and secondary. In the example on the left, the primary unit is active and passing traffic. The secondary unit is functioning as the standby unit. In the example on the right, the primary failed. The secondary became active and passes the data.

Hardware Failover: Active/Active

Cisco.com

Contexts

Primary: **1** **2** **1** **2** Secondary:

Active/**Standby** **Standby**/**Active**

Internet

Primary: **1** **2** **1** **2** Secondary:

Failed/**Standby** **Active**/**Active**

Internet
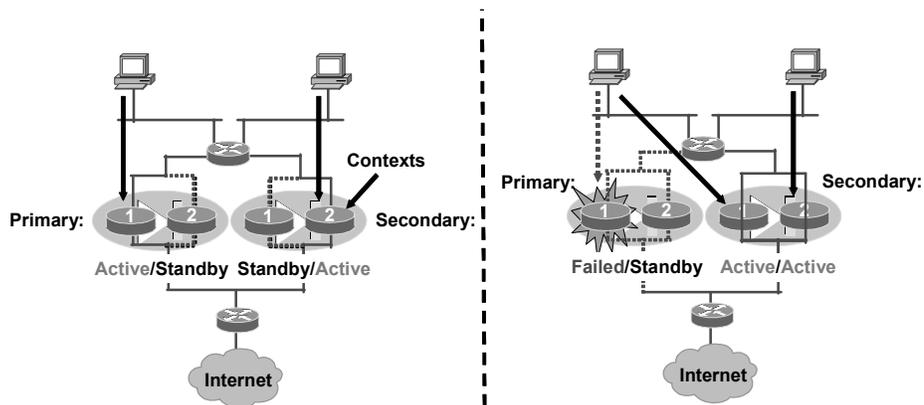
Hardware failover protects the network should the primary go offline.

• **Active/Active: Both units can process traffic and serve as backup units.**

SNPA v4.0—16-5

In active/active hardware failover, an administrator logically divides a security appliance into multiple contexts. Each security appliance can process traffic and serve as a backup unit. In the example on the left in the figure, each security appliance is composed of two contexts. Under normal conditions, each security appliance has one active and one standby context. Each active context processes approximately 50 percent of the traffic load while the other context is a standby unit for a context in the other security appliance.

In the active/active example on the right in the figure, the primary security appliance failed. The former standby context in the secondary security appliance transitioned to the active state. Now both contexts in the secondary security appliance are active (active/active). The security appliance on the right now handles 100 percent of the traffic, using both contexts.

Failover Requirements
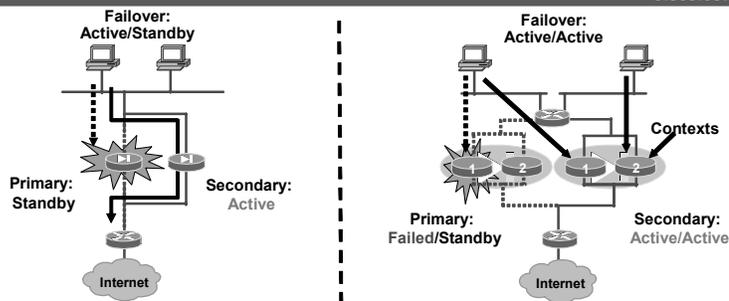
The primary and secondary security appliances must be identical in the following requirements:

- Same model number and hardware configurations
- Same software versions*
- Same features (DES or 3DES)
- Same amount of Flash memory and RAM
- Proper licensing

* Starting in version 7.0, the software versions do not have to be identical.

SNPA v4.0—16-6

The Cisco PIX Security Appliance 515/515E, 525, 535, and the Adaptive Security Appliance 5510, 5520, and 5540 can be used for failover. In order for failover to work, a pair of security appliances must be identical in the following requirements:

- **Platform type:** A Cisco PIX 515E Security Appliance cannot be paired with a Cisco PIX 515 Security Appliance.

- **Number and types of interfaces**

- **Software version:** For PIX Security Appliance Version 6.3 and earlier, software versions must be identical. Starting with Security Appliance Version 7.0 and later, the versions between failover pairs do not need to be the same. This enables an administrator to upgrade the operating software of the standby unit while the other member of the failover pair is active. Both security appliances must be a minimum of Security Appliance Version 7.0(1).

- **Licensed features:** Types of encryption, number of contexts, number of virtual private network (VPN) peers, and so forth.

- **Flash memory**

- **Amount of RAM**

- **Proper licensing:** The primary PIX Security Appliance failover units must have an unrestricted license (UR), while the secondary can have a UR or a failover license (FO). The PIX Security Appliance FO license can be either an active/standby only or an active/active failover only. To perform active/active failover on a PIX Security Appliance with a failover license, the FO license must be an active/active-only FO license. A restricted license cannot be used for failover, and two units with FO licenses cannot be used as a failover pair.

Note   Neither the Cisco PIX 501 Security Appliance nor the Cisco PIX 506E Security Appliance can be used for failover.

- **Link Up/Down test: Testing the network interface card itself**
- **Network Activity test: Testing received network activity**
- **ARP test: Reading the security appliance's ARP cache for the ten most recently acquired entries**
- **Broadcast Ping test: Sending out a broadcast ping request**

SNPA v4.0—16-7

Both the primary and secondary security appliances send special failover hello packets to each other over all network interfaces and the failover cable every fifteen seconds (the default), to make sure that everything is working. When a failure occurs in the active security appliance, and the failure is not caused by a loss of power in the standby security appliance, failover begins a series of tests to determine which security appliance has failed. The purpose of these tests is to generate network traffic to determine which, if either, security appliance has failed.

At the start of each test, each security appliance clears its received packet count for its interfaces. At the conclusion of each test, each security appliance looks to see if it has received any traffic. If it has, the interface is considered operational. If one security appliance receives traffic for a test and the other security appliance does not, the security appliance that did not receive traffic is considered failed. If neither security appliance has received traffic, the tests then continue.

The following are the four different tests used to test for failover:

- **LinkUp/Down:** This is a test of the network interface card itself. If an interface card is not plugged into an operational network, it is considered failed; for example, the hub or switch has failed, the network has a failed port, or a cable is unplugged. If this test does not find anything, the network activity test begins.

- **Network Activity:** This is a test of received network activity. The security appliance counts all received packets for on interval of up to five seconds. If any packets are received at any time during this interval, the interface is considered operational and testing stops. If no traffic is received, the ARP test begins.

- **ARP:** The Address Resolution Protocol (ARP) test consists of reading the ARP cache of the security appliance for the ten most recently acquired entries. The security appliance sends ARP requests one at a time to these machines, attempting to stimulate network traffic. After each request, the security appliance counts all received traffic for up to five seconds. If traffic is received, the interface is considered operational. If no traffic is received, an ARP request is sent to the next machine. If at the end of the list no traffic has been received, the ping test begins.

- **Broadcast Ping:** The ping test consists of sending out a broadcast ping request. The security appliance then counts all received packets for up to five seconds. If any packets are received at any time during this interval, the interface is considered operational and testing stops. If no traffic is received, the interface is considered failed.

Types of Failover Links

Primary Security Appliance
192.168.0.0 /24   10.0.0.0 /24

Internet

.1   e0   e1   .11
                    e3
              e2

Cable-Based →   ← Stateful
                                   Link
LAN-Based →   e2
                         e3
        e0   e1

Secondary Security Appliance

LAN-Based

Cable-Based

Stateful

SNPA v4.0—16-8
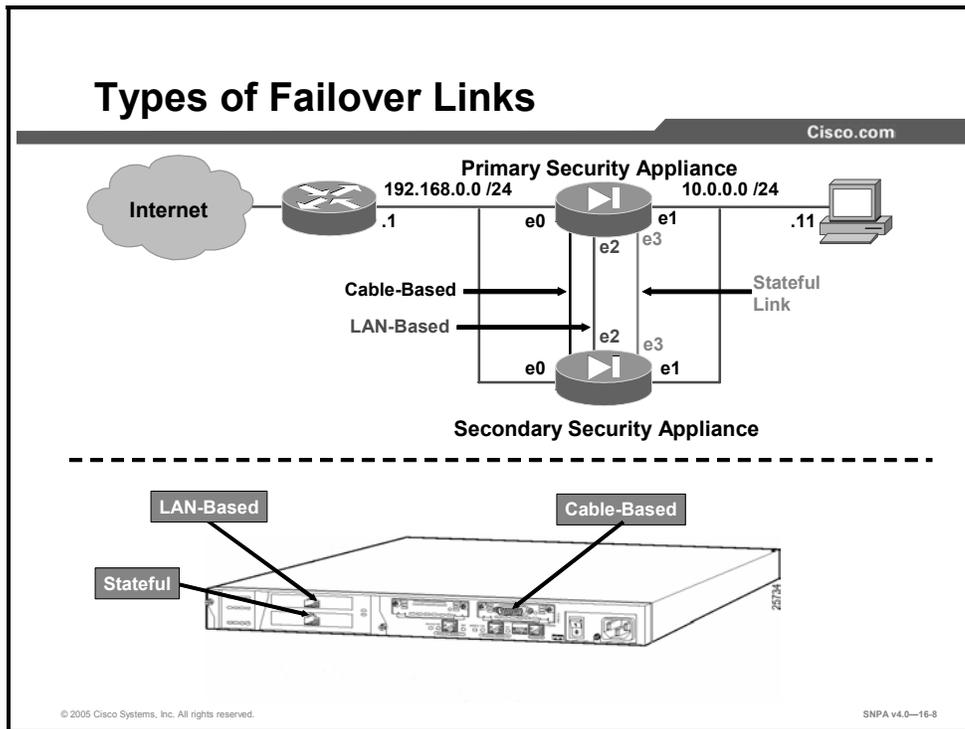
The security appliances communicate failover information between themselves. The communication identifies the unit as primary or secondary, identifies the power status of the other unit, and serves as a link for various failover communications between the two units. The majority of the failover communications are passed over dedicated failover links. The following are the three types of failover links:

■ **Serial failover cable:** The serial failover cable is a modified RS-232 serial link cable that transfers data at 115 kbps. (Not supported on the ASA Security Appliance.)

■ **LAN-based failover cable:** Cisco PIX Security Appliance Software Version 6.2 introduced support for LAN-based failover, so a special serial failover cable is no longer required to connect the primary and secondary security appliances. LAN-based failover overcomes the distance limitations imposed by the six-foot length of the serial failover cable. With LAN-based failover, failover messages are transmitted over Ethernet connections. Starting with Cisco PIX Security Appliance Version 7.0, serial cable failover also supports message encryption. LAN-based failover provides message encryption and authentication using a manual pre-shared key for added security. LAN-based failover requires an additional Ethernet on each security appliance to be used exclusively for passing failover communications between two security appliance units. The LAN failover interface can be connected to either a 100BASE-TX or 1000BASE-TX full duplex on a dedicated switch or dedicated VLAN of a switch. In PIX Security Appliance Version 7.0, it can also be a crossover Ethernet cable on the PIX Security Appliance platform and straight or crossover cable on the Adaptive Security Algorithm (ASA) platform. Data is passed over the dedicated interface using IP protocol 105. No hosts or routers should be on this interface.

- **Stateful failover cable:** The stateful failover cable passes per-connection stateful information to the standby unit. Stateful failover requires an additional Ethernet interface on each security appliance with a minimum speed of 100 Mbps full duplex to be used exclusively for passing state information between the two security appliance units. The stateful failover interface can be connected to either a 100BASE-T or 1000BASE-TX full duplex on a dedicated switch or dedicated VLAN of a switch. Starting with Version 7.0, the cable can also be a crossover Ethernet cable.

Serial Cable-Based Failover Configuration

This topic describes how to configure serial cable-based failover.

Serial Cable: Active/Standby Failover

Cisco.com

Primary: Active
Security Appliance

Internet — 192.168.2.2 — 10.0.2.1

Serial
Cable

192.168.2.7 — 10.0.2.7
Secondary: Standby
Security Appliance

Failover

Primary: Failed
Security Appliance

Internet — 192.168.2.7 — 10.0.2.7

Serial
Cable

192.168.2.2 — 10.0.2.1
Secondary: Active
Security Appliance

SNPA v4.0—16-10
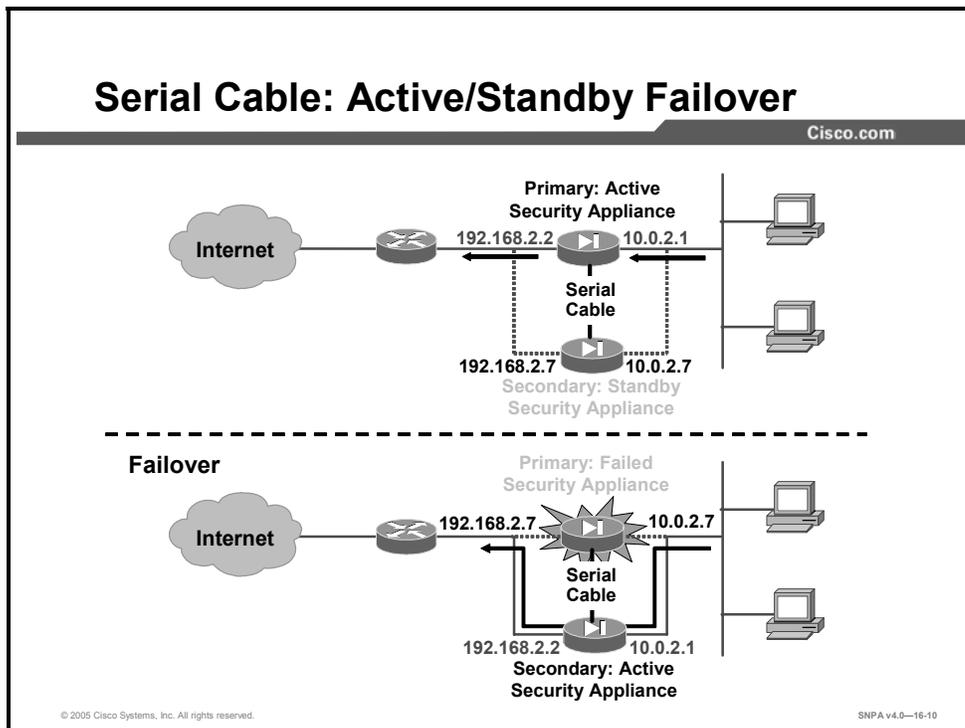
Serial cable-based failover is supported on the PIX Security Appliance only. In serial cable-based active/standby failover, there are two security appliances interconnected with a serial failover cable: a primary unit and a secondary unit. In the top example in the figure, the primary security appliance is active and passes traffic. The IP addresses of the outside and inside interfaces are 192.168.2.2 and 10.0.2.1. The secondary unit is standby and has interface IP addresses of 192.168.2.7 and 10.0.2.7. In the bottom example in the figure, the primary security appliance failed. In the active/standby application, the type of failover unit did not change; the primary unit is still the primary unit. What changed are the roles: active, standby, failed, and the interface IP addresses. The primary unit is now the failed unit. The secondary unit is now the active unit passing the traffic. The interface IP addresses were swapped. The secondary unit inherited the IP addresses of the primary unit, 192.168.2.2 and 10.0.2.1.

The benefits of using cable-based failover include the following:

- The PIX Security Appliance can immediately detect a power loss on the peer unit, and differentiate a power loss from an unplugged cable.

- The standby unit can communicate with the active unit and can receive the entire configuration without having to be bootstrapped for failover. In LAN-based failover, you need to configure the failover link on the standby unit before it can communicate with the active unit.

- The switch between the two units in LAN-based failover can be another point of hardware failure; cable-based failover eliminates this potential point of failure.

- You do not have to dedicate an Ethernet interface (and switch) to the failover link.

- The cable determines which unit is primary and which is secondary, eliminating the need to manually enter that information in the unit configurations.

The disadvantages of using cable-based failover include the following:

- Distance limitation—the units cannot be separated by more than six feet.
- Slower configuration replication.

Complete the steps below to configure failover with a serial failover cable. Important details for these steps follow. Before starting this procedure, if you have already powered it on, power off the standby security appliance and leave it off until instructed to power it on.

Step 163   Attach the security appliance network interface cables.

Step 164   Connect the serial failover cable between the primary and secondary security appliances.

Step 165   Configure the primary security appliance for failover and save the configuration to Flash memory.

Step 166   Power on the secondary security appliance and type the failover command, if failover is not enabled.

Step 1: Cable the Secondary Security Appliance
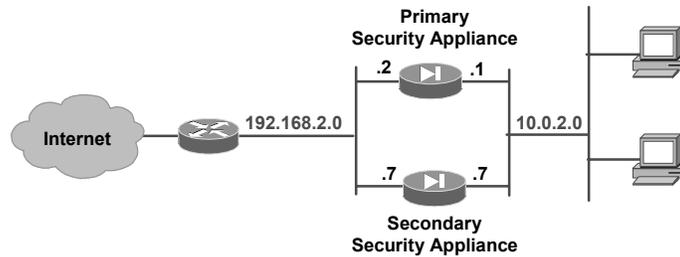
The steps to configure failover with a serial failover cable, in detail, are as follows:

Step 167 After verifying that the secondary security appliance is powered off, attach a network cable for each network interface you plan to use. Shut down any unused interfaces. The IP addresses on the secondary unit are different from the primary unit, but should be in the same subnet for each interface. If you plan to do stateful failover, one Ethernet interface on each security appliance must be dedicated to stateful failover.

Note Both units require the same access to all networks—inside, outside, Demilitarized Zone (DMZ), and so on. The primary and secondary security appliances must be on the same subnets for mutual networks (inside, outside, DMZ, partnernet, and so on).

Step 2: Connecting the Failover Cable

Primary
Security Appliance

Secondary
Security Appliance

Primary
Labeled
Connector

Secondary
Labeled
Connector
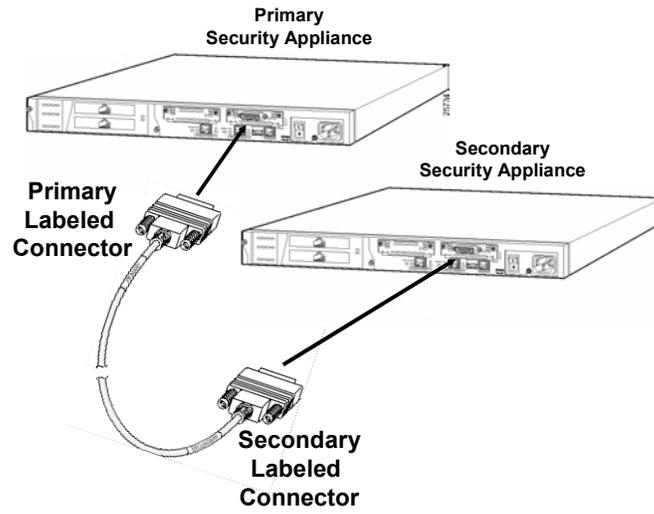
SNPA v4.0—16-13

Step 168 Connect the serial failover cable to the primary security appliance, ensuring that the end of the cable marked Primary attaches to the primary security appliance and that the end marked Secondary connects to the secondary security appliance. Do not power on the secondary security appliance.

Note   The cable itself determines the assignment of the primary and secondary failover unit.

Step 3: Configuring the Primary Security Appliance

Cisco.com

Primary
fw1

.2 .1

192.168.2.0

Internet

Failover
cable

10.0.2.0

.7 .7

Secondary
Security Appliance
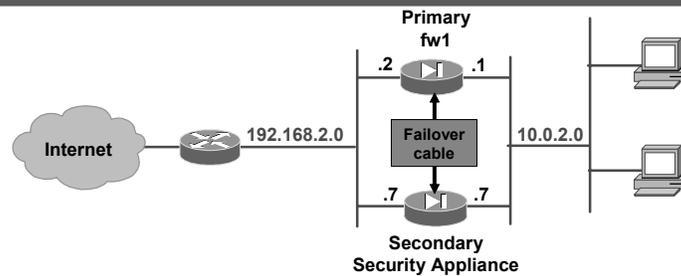
- **Enable failover on the primary security appliance.**
- **Create active and standby IP addresses on the primary security appliance.**
- **(Optionally) Set the failover polltime.**

```
fw2(config)# failover
fw2(config)# interface ethernet0
fw2(config-if)# ip address 192.168.2.2 255.255.255.0 standby 192.168.2.7 fw2(config)#
interface ethernet1
fw2(config-if)# ip address 10.0.2.1 255.255.255.0 standby 10.0.2.7
fw2(config)# failover polltime unit 10
```

SNPA v4.0—16-14

Step 169   Configure the primary security appliance as follows:

10. Use the **ip address** command to enter a standby IP address for each interface. These IP addresses are used by the standby security appliance and are different from the active security appliance addresses, but they should be in the same subnet for each interface.

11. If you are configuring stateful failover, use the **failover link** and **failover interface ip** commands to specify the name and IP addresses of a dedicated stateful failover interface.

12. If you want failover to occur faster, use the **failover polltime unit** command to set a time shorter than fifteen seconds for the security appliances to exchange hello packets, unit to unit. The **failover polltime unit** command sets how often hello messages are sent on the failover link. With a faster poll time, the security appliance can detect failure and trigger failover faster. However, faster detection may cause unnecessary switchovers when the network is temporarily congested or a network card starts slowly. The default, maximum, failover poll time is fifteen seconds. The minimum unit poll time value is one second. The security appliance will hold or wait for the failover hold time (three consecutive poll failures) before declaring the peer unit failed and triggering a failover.

13. Use the **failover** command to enable failover on the primary security appliance.

The table shows the syntax for the failover configuration commands.

```
failover link if_name [phy_if]
failover interface ip if_name statefu_link_primary_ip netmask standby
stateful_link_secondary_ip
failover polltime [unit] [msec] time [holdtime time]
failover polltime interface time
```

active	Makes a security appliance the active security appliance. Use this command when you need to force control of the connection back to the unit you are accessing, such as when you want to switch control back from a security appliance after you have fixed a problem and want to restore service to the primary security appliance.
if_name	Specifies the interface name for the failover IP address.
phy_if	Specifies the physical interface name.
link	Specifies the interface where a fast LAN link is available for stateful failover.
if_name	Specifies a dedicated fast LAN link for stateful failover.
holdtime *time*	(Optional) Sets the time during which a unit must receive a hello message on the failover link, after which the peer unit is declared failed. Valid values range from 3 to 45 seconds.
interface *time*	Specifies the poll time for interface monitoring. Valid values range from 3 to 15 seconds.
polltime *time*	Specifies how long failover waits before sending special failover hello packets between the primary and standby security appliances over all network interfaces and the failover cable. The default is 15 seconds. The minimum value is 1 second and the maximum is 15 seconds. Set the time to a lower value for stateful failover. With a faster poll time, the security appliance can detect failure and trigger failover faster. However, faster detection may cause unnecessary switchovers when the network is temporarily congested or a network card starts slowly.

14. Set the clock. The security appliance clock is stored in the CMOS. Specify the **clock set** command on the active security appliance to synchronize the time on both security appliances.

15. Use the **write memory** command to save the configuration to Flash memory. Configure only the primary security appliance.

By default, a single interface failure causes failover. You can control which interfaces are monitored for failover. By default, monitoring of physical interfaces is enabled and monitoring of subinterfaces is disabled. You can monitor up to 250 interfaces on a unit. You can control which interfaces affect your failover policy by disabling the monitoring of specific interfaces and enabling the monitoring of others. This lets you exclude interfaces attached to less critical networks from affecting your failover policy.

To disable health monitoring for an interface, enter the following command in global configuration mode:

monitor-interface *if_name*

You can change the number of interfaces that must fail before a failover occurs. The default is a failure of one interface (interface policy of "1"). To change the default failover criteria, enter the following command in global configuration mode:

failover interface-policy num[%]

When specifying a specific number of interfaces, the *num* argument can be from 1 to 250.

show failover Command: Secondary Security Appliance Powered Off

```
fw2# show failover
Failover On
Cable status: Other side not connected
Failover unit Primary
Failover LAN Interface: N/A  - Serial-based failover enabled
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 3 of 250 maximum
Last Failover at: 13:21:38 UTC Dec 10 2004
        This host: Primary - Active
                Active time: 200 (sec)
                Interface outside (192.168.2.2): Normal (Waiting)
                Interface inside (10.0.2.1): Normal (Waiting)
                Interface dmz (172.16.2.1): Normal (Waiting)
        Other host: Secondary - Not detected
                Active time: 0 (sec)
                Interface outside (192.168.2.7): Unknown (Waiting)
                Interface inside (10.0.2.7): Unknown (Waiting)
                Interface dmz (172.16.2.7): Unknown (Waiting)

Stateful Failover Logical Update Statistics
        Link : Unconfigured
```

SNPA v4.0—16-15

Use the **show failover** command to view the failover status. The **show failover** command provides the following information:

- Status of failover

- Cable status

- Unit poll frequency

- Interface poll frequency

- Interface (failure) policy

- Monitored interfaces

- Primary and secondary unit status

- Primary and secondary interface status

In the example in the figure, notice that failover is on, cable status is not connected to the other side, and this is the primary security appliance. The security appliances are using serial-based failover with a poll interval of 15 seconds and a hold time of 45 seconds. The interface policy is set to one; one failed interface causes a failover. The number of monitored interfaces is 3: inside, outside, and dmz interfaces. The secondary unit is still powered down.

In the bottom half of the example, notice the types of failover units and their status. This security appliance is the primary failover unit and its status is active. The secondary unit is not detected. Notice the IP addresses of the primary and secondary units. The outside interface address on the primary unit is 192.168.2.2, and the address of the outside interface of the secondary unit is 192.168.2.7. The primary unit interfaces are normal (waiting), and the secondary unit interfaces are unknown (waiting). The secondary unit is powered off and there is no communication between units. The following table provides the administrator with a description of the **show failover** command statistics:

Statistic	Description
Failover	• On • Off
Cable status:	• Normal—The cable is connected to both units, and they both have power. • My side not connected—The serial cable is not connected to this unit. It is unknown if the cable is connected to the other unit. • Other side is not connected—The serial cable is connected to this unit, but not to the other unit. • Other side powered off—The other unit is turned off. • N/A—LAN-based failover is enabled.
Failover unit	Primary or Secondary.
Failover LAN interface	Displays the logical and physical name of the failover link.
Unit poll frequency	Displays the number of seconds between hello messages sent to the peer unit and the number of seconds during which the unit must receive a hello message on the failover link before declaring that the peer failed.
Interface poll frequency	*n* seconds. The number of seconds you set with the **failover polltime interface** command. The default is 15 seconds.
Interface policy	Displays the number or percentage of interfaces that must fail to trigger failover.
Monitored interfaces	Displays the number of interfaces monitored out of the maximum possible.
failover replication http	Displays if HTTP state replication is enabled for stateful failover.
Last failover at:	The date and time of the last failover in the following form: hh:mm:ss UTC DayName Month Day yyyy UTC (Coordinated Universal Time) is equivalent to GMT (Greenwich Mean Time).
This host: Other host:	For each host, the display shows the following information.
Primary or Secondary	• Active • Standby
Active time:	*n* (sec). The amount of time the unit has been active. This time is cumulative, so the standby unit, if it was active in the past, will also show a value.

Interface name (n.n.n.n):	For each interface, the display shows the IP address currently being used on each unit, as well as one of the following conditions: • Failed—The interface has failed. • No Link—The interface line protocol is down. • Normal—The interface is working correctly. • Link Down—The interface has been administratively shut down. • Unknown—The security appliance cannot determine the status of the interface. • Waiting—Monitoring of the network interface on the other unit has not yet started.
Stateful Failover Logical Update Statistics	The following fields relate to the stateful failover feature. If the Link field shows an interface name, the stateful failover statistics are shown.

Configuration Replication

Primary Security Appliance

Internet

Replication

Secondary Security Appliance
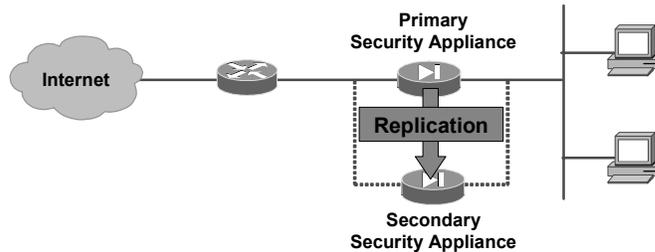
Configuration replication occurs:

- **When the standby firewall completes its initial bootup**
- **As commands are entered on the active firewall**
- **By entering the** write standby **command**

SNPA v4.0—16-16

Configuration replication is the configuration of the primary security appliance being replicated to the secondary security appliance. To perform configuration replication, both the primary and secondary security appliances must be exactly the same and run the same software release (not required starting with Security Appliance Version 7.0). The configuration can be replicated from the active security appliance to the standby security appliance in these three ways:

- When the standby security appliance completes its initial bootup, the active security appliance replicates its entire configuration to the standby security appliance.

- As commands are entered on the active security appliance, they are sent across the failover cable to the standby security appliance.

- Entering the **write standby** command on the active security appliance forces the entire configuration in memory to be sent to the standby security appliance.

Configuration replication occurs only from memory to memory. Because this is not a permanent place to store configurations, you must use the **write memory** command to write the configuration into Flash memory. Entering **write memory** on the active unit will result in both security appliances saving the configuration to Flash memory.

When replication starts, the security appliance console displays the message "beginning configuration replication to mate," and when replication is complete, displays the message "end configuration replication to mate." During replication, information should not be entered on the security appliance console. Replication may take some time to complete with failover for a large configuration because configuration replication occurs over the serial failover cable.

Note	Changes made on the standby unit are not replicated to the active unit.

Step 4: Powering on the Secondary Firewall

Cisco.com

Primary
fw1

.2 .1

Internet 192.168.2.0 Replication 10.0.2.0

.7 .7

Secondary
Security Appliance

Power
On
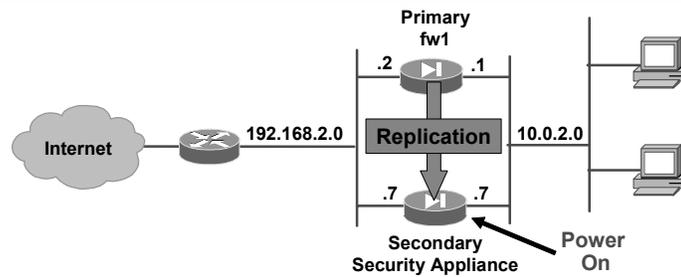
- **Replication of primary security appliance to secondary security appliance**

```
 Detected an active mate
Beginning configuration replication to mate.
End configuration replication to mate.
```

SNPA v4.0—16-17

Step 170   Power on the secondary security appliance. When the secondary security appliance completes its initial bootup, the primary security appliance recognizes it and starts synchronizing and replicating the configurations. As the configurations synchronize, the messages "beginning configuration replication to mate" and "end configuration replication to mate" appear on the primary unit.

Note   You need to use the **write memory** command on the active unit to save the replicated configuration on the standby unit.

show failover Command

```
         Detected an active mate
Beginning configuration replication to mate.
End configuration replication to mate.

fw2# show failover
Failover On
Cable status: Normal
Failover unit Primary
Failover LAN Interface: N/A  - Serial-based failover enabled
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 3 of 250 maximum
Last Failover at: 13:21:38 UTC Dec 10 2004
        This host: Primary - Active
                Active time: 300 (sec)
                Interface outside (192.168.2.2): Normal
                Interface inside (10.0.2.1): Normal
                Interface dmz (172.16.2.1): Normal
        Other host: Secondary – Standby Ready
                Active time: 0 (sec)
                Interface outside (192.168.2.7): Normal
                Interface inside (10.0.2.7): Normal
                Interface dmz (172.16.2.7): Normal

Stateful Failover Logical Update Statistics
        Link : Unconfigured
```

SNPA v4.0—16-18

Use the **show failover** command to check the status of the primary and secondary units after secondary unit powerup and replication is completed. Notice that the cable status (normal), the secondary unit (standby ready), and configured secondary interfaces (normal) have changed.

Force Control Back

Primary: ~~Standby~~ Active
fw1

Internet

192.168.0.0

10.0.0.0

Secondary: ~~Active~~ Standby
fw2
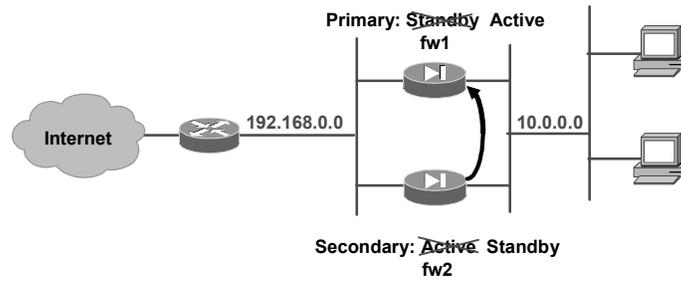
fw1(config)#

```
failover active
```

- **Forces control of the connection back to the unit you are accessing**

```
fw2(config)# failover active
```

SNPA v4.0—16-19

Use the **failover active** command when you need to force control of the connection back to the unit you are accessing, such as when you want to switch control back from a unit after you have fixed a problem and want to restore service to the primary unit. Either enter the **no failover active** command on the secondary unit to switch service to the primary or the **failover active** command on the primary unit.

The **failover reset** command forces both security appliances back to an unfailed state. This command can be entered from either security appliance, but it is best to always enter commands at the active security appliance. Entering the **failover reset** command at the active firewall unfails the standby firewall.

Active/Standby LAN-Based Failover Configuration

This topic describes how to configure LAN-based failover.

LAN-Based Failover Overview

LAN-based failover:

- **Provides long-distance failover functionality**
- **Uses an Ethernet cable rather than the serial failover cable**
- **Requires a dedicated LAN interface, but the same interface can be used for stateful failover**
- **Requires a dedicated switch, hub, or VLAN**
- **Uses message encryption and authentication to secure failover transmissions**

SNPA v4.0—16-21

LAN-based failover overcomes the distance limitations imposed by the six-foot failover cable. With LAN-based failover, an Ethernet cable can be used to replicate configuration from the primary security appliance to the secondary security appliance; the special serial failover cable is not required. Instead, LAN-based failover requires a dedicated LAN interface and a dedicated switch, hub, or switch VLAN. Prior to Version 7, you can not use a crossover Ethernet cable to connect the two security appliances for LAN-based failover.

The same LAN interface used for LAN-based failover can also be used for stateful failover. However, the interface needs enough capacity to handle both the LAN-based failover and stateful failover traffic. If the interface does not have the necessary capacity, use two separate, dedicated interfaces.

LAN-based failover allows traffic to be transmitted over Ethernet connections that are relatively less secure than the special failover cable; therefore, to secure failover transmissions, LAN-based failover provides message encryption and authentication using a manual pre-shared key.

Note	Starting with PIX Security Appliance Version 7.0, crossover Ethernet cable can also be used for LAN-based failover cabling. Straight and crossover cables can be used for ASA LAN-based failover cabling.

LAN-Based Failover Configuration Overview

Complete the following tasks to configure LAN-based failover:

1. Install a LAN-based failover connection between primary and secondary security appliances.
2. Configure the primary security appliance.
3. Configure the primary security appliance for stateful failover.
4. Save the primary security appliance configuration to Flash memory.
5. Power on the secondary security appliance.
6. Configure the secondary security appliance with the minimum failover LAN command set.
7. Save the secondary security appliance configuration to Flash memory.
8. Connect the secondary unit LAN failover interface to the network.
9. Reboot the secondary security appliance.

Complete the following steps to configure LAN-based failover:

Step 171 Install a LAN-based failover connection between security appliances. Verify that any switch port that connects to a security appliance failover link is configured to support LAN-based failover. Disconnect the secondary security appliance.

Step 172 Configure the primary security appliance for failover.

Step 173 Configure the primary security appliance for stateful failover.

Step 174 Save the configuration of the primary security appliance to Flash memory.

Step 175 Power on the secondary security appliance.

Step 176 Configure the secondary security appliance with the LAN-based failover command set.

Step 177 Save the configuration of the secondary security appliance to Flash memory.

Step 178 Connect the LAN-based failover interface of the secondary security appliance to the network.

Step 179 Reboot the secondary security appliance.

Cabling LAN Failover
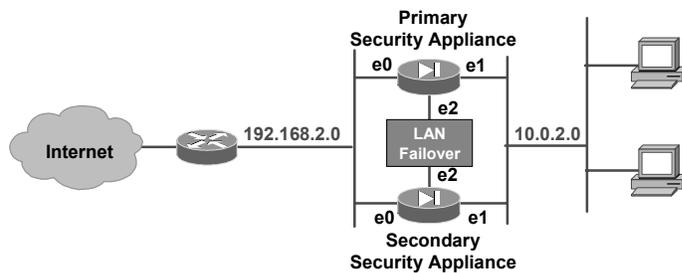
SNPA v4.0—16-23

The following steps provide more details about configuring LAN-based failover:

Step 180   Install a LAN-based failover connection between security appliances, as follows:

■   Attach a network cable for each network interface you plan to use. The host IP addresses on the secondary unit are different from the addresses on the primary unit, but they should be in the same subnet for each interface. If you plan to do stateful failover, one of the interfaces must be dedicated to this function (if not sharing the LAN-based failover connection). If the LAN failover cable is connected to the secondary security appliance, disconnect it.

■   Perform the following on any switch port that connects to these security appliances:

—   Enable PortFast.

—   Turn off channelling.

Configuring LAN Failover: Primary

Cisco.com
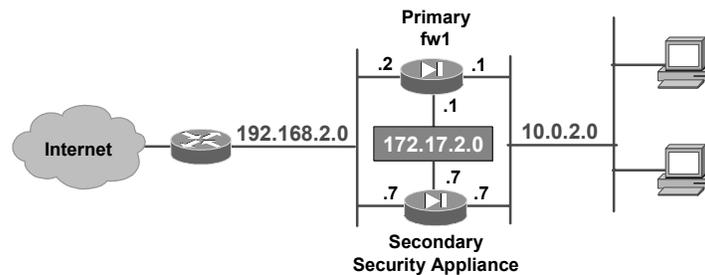
```
fw2(config)# interface ethernet3
fw2(config-if)# no shut
fw2(config)# failover lan interface LANFAIL ethernet3
fw2(config)# failover interface ip LANFAIL 172.17.2.1 255.255.255.0 standby 172.17.2.7
fw2(config)# failover lan enable
fw2(config)# failover lan unit primary
fw2(config)# failover key 1234567
fw2(config)# failover
```

SNPA v4.0—16-25

The following steps provide more details about configuring LAN-based failover:

Step 181 Complete the following substeps to configure the primary security appliance before connecting the failover LAN interface:

16. Use the **clock set** command on the active security appliance to synchronize the time on the primary and secondary security appliances.

17. Ensure that you have not used the **auto** or the **1000auto** option in any interface command in your configuration. If you have used one of these options, change it by reentering the command with the correct information. Always specify the speed for the interface, such as 10BASE-T for 10 Mbps or 100BASE-TX for 100 Mbps. Ensure that the speeds and duplexes are the same for any devices on the subnets, including switches and routers. For stateful failover, set the stateful failover dedicated interface speed to 100full or 1000full.

Note   Use the **clear xlate** command after changing the **interface** command.

---

18. Configure a dedicated LAN-based failover interface as follows:

■ Use the **interface** command and **no shut** subcommand to enable the interface.

■ Use the **failover lan interface** command to specify the interface used for failover communications.

■ Use the **failover interface ip** command to specify the active and standby IP addresses for the failover interface.

19. Use the **failover lan enable** command to enable LAN-based failover.

20. Use the **failover lan unit** command to configure the security appliance as the primary unit in a LAN failover configuration.

21. (optionally) Use the **failover key** command to specify the failover shared secret for encrypted and authenticated communication between failover pairs.

22. If you are configuring stateful failover, use the **failover link** and **failover interface ip** command to specify the name of the dedicated interface you are using.

23. Use the **failover** command to enable failover.

24. Connect the failover interface of the primary security appliance to the network.

25. Save the configuration of the primary security appliance to Flash memory.

The table shows the syntax of the **failover lan** commands.

```
failover lan unit primary | secondary
failover lan interface if_name phy_if
failover interface ip if_name statefu_link_primary_ip netmask standby
stateful_link_secondary_ip
failover key key_secret
failover lan enable
```

if_name	Specifies the interface name for LAN-based failover.
phy_if	Specifies the physical or logical interface port.
key	Enables encryption and authentication of LAN-based failover messages between security appliances.
key_secret	Specifies the failover encryption shared secret key.

Stateful Failover

Cisco.com

Primary
fw1

.1 .1

e2

Internet 192.168.2.0 Stateful failover 10.0.2.0

e2

.2 .2

Secondary
Security Appliance
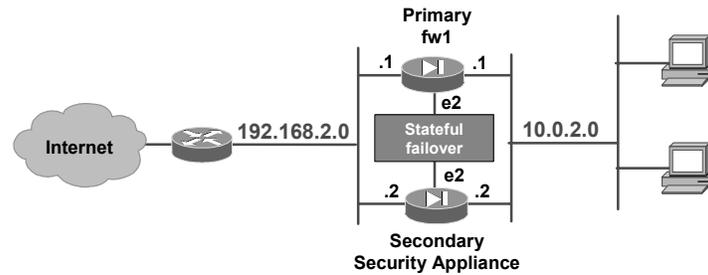
`fwfirewall(config)#`

```
failover link if_name [phy_if]
```

- **Specifies the name of the dedicated interface used for stateful failover.**

```
fw2(config)# failover link LANFAIL
```

SNPA v4.0—16-26

The following step provides more details about configuring the failover link:

Step 182 The stateful failover feature passes per-connection stateful information to the standby unit. After a failover occurs, the same connection information is available at the new active unit. End-user applications are not required to do a reconnect to keep the same communication session. The state information passed to the standby unit includes the global pool addresses and status; connection and translation information and status; the negotiated H.323, SIP, and MGCP UDP ports; the port allocation bit map for PAT; and other details necessary to let the standby unit take over processing if the primary unit fails.

Depending on the failure and failover holdtime, the security appliance switchover times will vary. Applications not handled by stateful failover will then require time to reconnect before the active unit becomes fully functional.

The same LAN interface used for LAN-based failover can also be used for stateful failover. However, the interface needs enough capacity to handle both the LAN-based failover and stateful failover traffic. If the interface does not have the necessary capacity, use two separate, dedicated interfaces.

Stateful failover requires an Ethernet interface with a minimum speed of 100 Mbps full duplex to be used for passing state information between the two security appliance units. The stateful failover interface can be connected with the following:

- 100Base-TX full duplex on a dedicated switch or dedicated VLAN of a switch

- 1000Base-SX full duplex on a dedicated switch or dedicated VLAN of a switch

- Crossover cable on PIX Security Appliance starting with PIX Security Appliance Version 7.0

- Straight or crossover LAN cable on ASA security appliance

The state information passed to the standby unit includes the following:

- Network Address Translation (NAT) table

- TCP connection states

- UDP connection states

- The ARP table

- The Layer 2 bridge table (when running in transparent security appliance mode)

- The HTTP connection states (when HTTP replication is enabled)

- The Internet Security Association and Key Management Protocol (ISAKMP) and IPSec security association (SA) table

The information that is not passed to the standby unit when stateful failover is enabled includes the following:

- The HTTP connection table (when HTTP replication is disabled)

- The user authentication (uauth) table

- The routing tables

Data is passed over the dedicated failover interface using IP Protocol 8 or 9. No hosts or routers should be on this interface.

Step 183   Save the primary security appliance to Flash memory.

Configuring LAN Failover: Secondary

Cisco.com
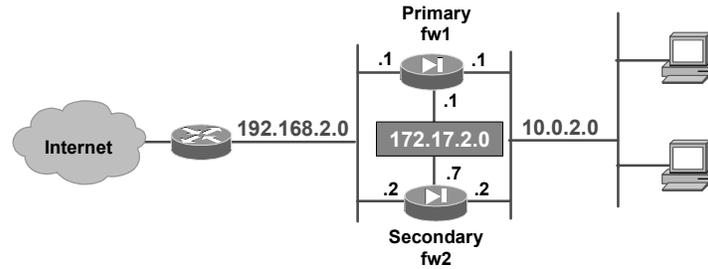
```
fw2(config)# interface ethernet3
fw2(config-if)# no shut
fw2(config)# failover lan interface LANFAIL ethernet3
fw2(config)# failover interface ip LANFAIL 172.17.2.1 255.255.255.0 standby 172.17.2.7
fw2(config)# failover lan unit secondary
fw2(config)# failover lan key 1234567
fw2(config)# failover lan enable
fw2(config)# failover
```

SNPA v4.0—16-28

After the primary security appliance is configured, configure the secondary security appliance. The following describes the steps necessary to configure the secondary security appliance to support failover:

Step 184 Power on the secondary security appliance.

Step 185 Without the secondary unit LAN-based failover interface connected, configure a LAN-based failover interface for a dedicated secondary unit as follows:

- Use the **interface** command and **no shut** subcommand to enable the interface.

- Use the **failover lan interface** command to specify the interface used for failover communications.

- Use the **failover interface ip** command to specify the active and standby IP address for the failover interface.

- Use the **failover lan unit** command to designate this security appliance as the secondary security appliance.

- (optional) Use the **failover key** command to enter the secret key shared with the primary security appliance.

- Use the **failover lan enable** command to enable LAN-based failover.

- Use the **failover** command to enable failover.

Step 186 Use the **write memory** command to save your configuration to Flash memory.

In the figure, all the **failover lan** commands are entered on the secondary security appliance exactly as they would be entered on the primary, except the **failover lan unit secondary** command. On both security appliances, "ethernet3" is designated as the LAN failover interface and is configured with the following parameters:

- Name: LANFAIL
- IP address: 172.17.2.1
- Netmask: 255.255.255.0
- Standby IP address: 172.17.2.7
- Failover LAN key: 1234567

The output of the **show failover interface** command details LAN-based failover interface IP addressing. The following is an example of the primary unit **show failover** command output:

```
fw2(config)# show failover interface
        interface lanfail Ethernet3
                System IP Address: 172.17.2.1 255.255.255.0
                My IP Address    : 172.17.2.1
                Other IP Address : 172.17.2.7
```

Replication to Secondary
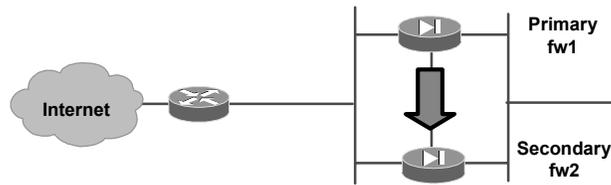
Once the secondary security appliance is configured for failover, the following steps are used to replicate the configuration form the primary to the secondary security appliance.

Step 187 Connect the failover interface of the secondary security appliance to the network.

Step 188 Use the **reload** command to reboot the secondary security appliance. The primary security appliance configuration is replicated on the secondary security appliance. The following messages will appear on the primary security appliance: "Beginning configuration replication: Sending to mate", which denotes the start of the synchronization, and "End Configuration replication to mate", which acknowledges the completion of the replication.

You need to enter **write memory** command on the active unit to save the replicated configuration on the standby unit.

show failover Command with LAN-Based Failover

```
fw2(config)# sh fail
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Secondary
Failover LAN Interface: lanfail Ethernet3 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 3 of 250 maximum
Last Failover at: 18:03:38 UTC Nov 12 2004
        This host: Primary - active
                Active time: 375 (sec)
                Interface outside (192.168.2.2): Normal (Waiting)
                Interface inside (10.0.2.1): Normal (Waiting)
                Interface dmz (172.16.2.1): Normal (Waiting)
        Other host: Secondary – Standby Ready
                Active time: 3795 (sec)
                Interface outside (192.168.2.7): Normal (Waiting)
                Interface inside (10.0.2.7): Normal (Waiting)
                Interface dmz (172.16.2.7): Normal (Waiting)
```

SNPA v4.0—16-30

The figure shows the output of the **show failover** command after replication. It includes a section for LAN-based failover, which displays the name and IP address of the interface used for LAN-based failover. Notice that this interface does not appear in the interface list that displays the status of the interfaces.

failover mac address Command

Outside MAC address
Act - 00a0.c989.e481
Stby - 00a0.c969.c7f1

Primary
fw1

Inside MAC address
Act - 00a0.c976.cde5
Stby - 00a0.c922.9176

.1   .1

Internet   192.168.2.0   10.0.2.0

.2   .2
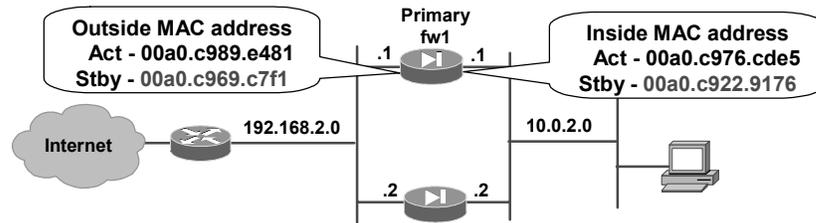
```
fw1(config)#
failover mac address mif_name act_mac stn_mac
```

• **Enables you to configure a virtual MAC address for a security appliance failover pair.**

```
fw2(config)# failover mac address ethernt0 00a0.c989.e481
  00a0.c969.c7f1
fw2(config)# failover mac address ethernet1 00a0.c976.cde5
  00a0.c922.9176
```

SNPA v4.0—16-31

When the primary security appliance is replaced with a new primary security appliance, the secondary security appliance acquires the MAC address of the new primary security appliance and sends out gratuitous ARPs on all interfaces to update the devices connected to the security appliance. You can prevent the MAC address change by manually setting the MAC addresses of the primary and secondary security appliance using the command **failover mac address**. With LAN-based failover, the security appliance can be configured to use a virtual MAC address instead of assuming the MAC address of its failover peer. If a virtual MAC address is not specified, the security appliance failover pair uses the burned-in network interface card address as the MAC address.

When adding the **failover mac address** command to your configuration, it is best to configure the virtual MAC address, save the configuration to Flash memory, and then reload the security appliance pair. You must also write the complete security appliance configuration, including the **failover mac address** command, into the Flash memory of the secondary security appliance for the virtual MAC addressing to take effect.

The syntax of the **failover mac address** command is as follows:

failover mac address *phy_if act_mac stn_mac*

phy_if	Specifies the name of the interface to set the MAC address.
act_mac	Specifies the interface MAC address for the active security appliance.
stn_mac	Specifies the interface MAC address for the standby security appliance.

Note   If the virtual MAC address is added when there are active connections, those connections drop.

Note	The **failover mac address** command is unnecessary on an interface configured for LAN-based failover because the **failover lan interface** command does not change the IP and MAC addresses when failover occurs.

Active/Active Failover Configuration

This topic describes how active/active failover works and how to configure it.
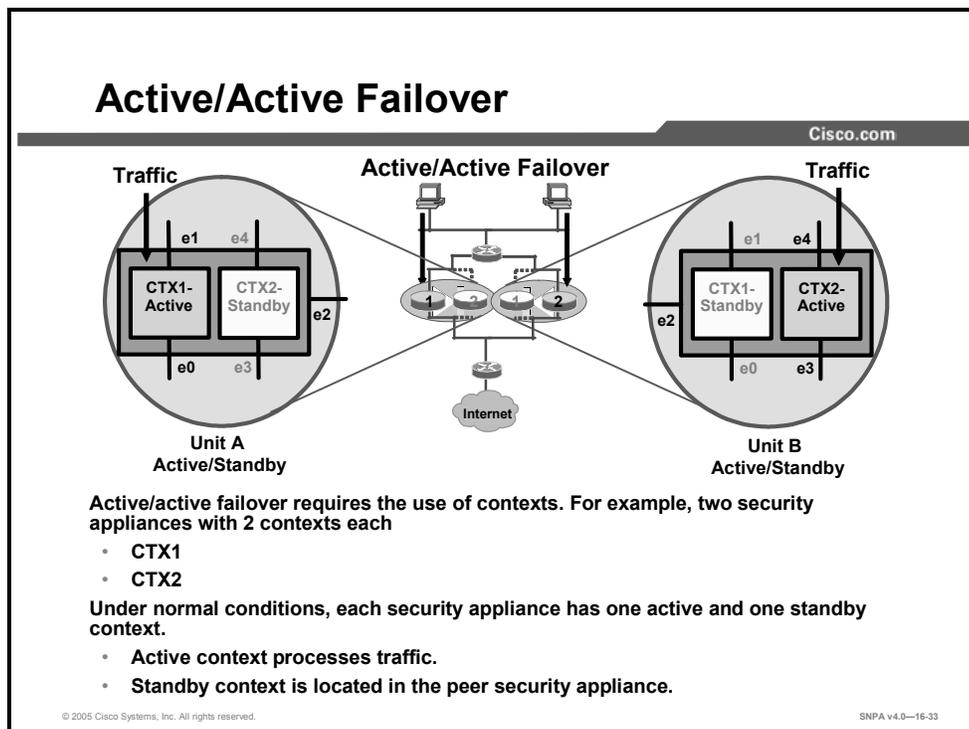
Under the active/standby failover model, only one security appliance actively processes user traffic while the other unit acts as a hot standby, prepared to take over if the active unit fails. Cisco PIX Security Appliance and ASA Security Appliances software release 7.0 adds the capability of active/active failover. When two security appliances are configured to function in active/active failover, both units can actively process security appliance traffic while at the same time serving as a back up for their peer unit.

The active/active failover feature leverages the virtual context feature. In the example in the figure, there are two security appliances configured for active/active failover, Unit A and Unit B. Each security appliance is partitioned into two contexts, CTX1 and CTX2. In the security appliance active/active scenario, under normal conditions, there is one active context and one standby context per unit. In Unit A, CTX1 is active and passing traffic. CTX1 in Unit B is in standby state. In Unit B, CTX2 is active and passing traffic while CTX2 in Unit A is in standby state. Under normal conditions, each unit handles 50 percent of the traffic. The security appliance active/active cluster itself does not perform load balancing. It is the responsibility of the administrator to engineer the network so that it routes 50 percent of the traffic to each unit. This can be accomplished either statically or with the use of an upstream router to do load balancing on the traffic.

Note   Serial cable failover can also be used for PIX Security Appliance active/active failover.

Active/Active Failover (Cont.)

Active/Active Failover

Traffic   Traffic

Unit A:
Failed/Standby

Unit B:
Active/Active

Under failed conditions, Unit A determines outside interface on CTX1 has failed.

- **CTX1 is placed in failed state.**
- **Unit A has one failed and one standby context.**

Unit B, CTX1 becomes active.

- **Unit B has two active contexts.**
- **Both active contexts pass traffic.**

Failover can be context-based or unit-based.

SNPA v4.0—16-34

In the previous example, in Unit A, CTX1 was active while CTX2 was standby. In Unit B, CTX1 was standby while CTX2 was active. Active/active failover logic enables each security appliance to determine whether a failure is context-based or unit-based. If an active context fails, the active context transitions to a failed state. In the peer security appliance, the standby context transitions from standby to active. For example, in the figure, if Unit A interface e0 fails, Unit A can determine that the failure is a context-based failure. Unit A places CTX1 in a failed state. Unit A can communicate with Unit B about the change in state of CTX1. Unit B changes the state of its CTX1 to active. After the state change, both of the Unit B contexts are active and passing traffic. Failover can be context-based or unit-based. When a failure affects the whole unit, the peer unit can take over by activating any standby contexts and start processing 100 percent of the traffic.

Configure Failover Link

Cisco.com
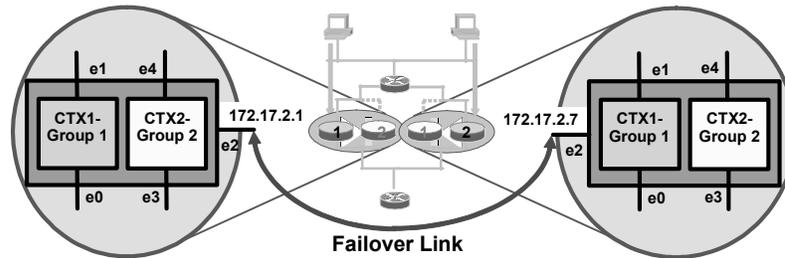
```
fw2(config)# interface ethernet2
fw2(config-if)# no shut
fw2(config)# failover lan interface LANFAIL ethernet2
fw2(config)# failover interface ip LANFAIL 172.17.1.1 255.255.255.0 standby 172.17.1.7
fw2(config)# failover lan enable
fw2(config)# failover link LANFAIL ethernet2
fw2(config)# failover lan key 1234567
```

SNPA v4.0—16-35

Failover link is used to communicate unit health, interface health, switchover messages, configuration re-synchronization, and so on. To configure active/active failover, both security appliances must be in multimode. The administrator configures the failover link in the system configuration of the primary failover unit. Before configuring the failover link, be sure that the failover link interface is not in administrative shutdown. In the example in the figure, the administrator configures both security appliances as follows:

■ Removes the failover link interface, interface e2, from administrative shutdown

■ Identifies the name of the failover link and the failover link interface

■ Configures the failover link IP address and standby address

■ Enables LAN-based failover

■ Enables stateful failover on LANFAIL link

■ Specifies the shared secret key for encrypted and authenticated communications between failover pairs

Do not enable failover until the failover groups are configured.

Failover Group

Primary

Group 2

Secondary

e1 e4

CTX1-
Group 1

CTX2-
Group 2

172.17.2.1

e2

e0 e3

e1 e4

172.17.2.7

CTX1-
Group 1

CTX2-
Group 2

e2

e0 e3

1 2 1 2
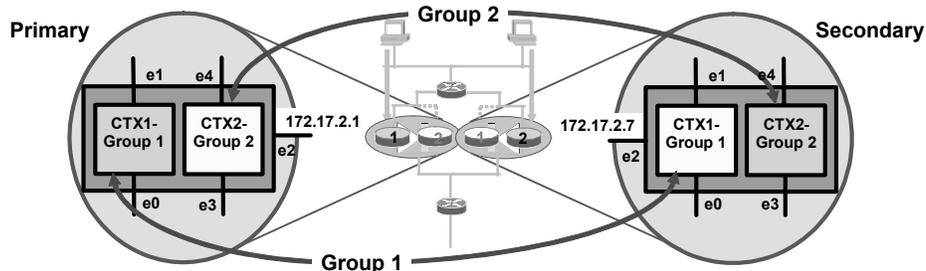
Group 1

- **Active/active failover adds support for failover group.**
- **Failover is performed on a unit or group level.**
- **A group is comprised of one or more contexts.**
- **Each failover group contains separate state machines to keep track of the group failover state.**

```
fw2(config)# failover group 1
fw2(config-fover-group)# primary
fw2(config)# failover group 2
fw2(config-fover-group)# secondary
```

　　　　　　　　　　　　　　　SNPA v4.0—16-36

In active/standby failover, failover is performed on a unit basis. One unit is active while the other unit is a standby unit. In active/active failover, failover is performed on a context basis. One context is active while the peer context is in standby state. ASA and PIX Security Appliance software release 7.0 introduces the concept of the failover group. Each security appliance supports up to two failover groups. You can join one or more contexts to a failover group. For example, context CTX1, CTX2, and CTX3 can join Group 1 while context CTX4 and CTX5 can join Group 2. The security appliance uses failover groups to manage contexts. Each failover group contains separate state machines to keep track of their context failover states. In the example in the figure, there are two failover groups, Group 1 and Group 2. Context CTX1 joins Group 1 and CTX2 joins Group 2. Group 1 monitors the health of CTX1 and Group 2 monitors the health of CTX2 across both security appliances. Failover can occur on a group or system basis.

You can configure failover Group 1 and Group 2 attributes using the **failover group** command. The **failover group** command can only be added while the administrator is in multimode system configuration and failover is disabled.

Entering the **failover group** command places you in the failover group subcommand mode. The **primary**, **secondary**, **preempt**, **replication http**, **interface-policy**, and **polltime interface** commands are available in the failover group subcommand mode. Use the **exit** command to return to global configuration mode.

The syntax for the failover group command is as follows:

failover group num
primary|secondary
preempt [*<preempt_delay_in_seconds>*]
replication http
polltime interface *<seconds>*
interface-policy *N[%]*
mac address *<phyifc>* *<act_mac>* *<stn_mac>*

primary	Gives the primary unit higher priority.
secondary	Gives the secondary unit higher priority.
Polltime interface	Specifies interface polling interval.
preempt	Allows preemption of lower priority active unit.
replication http	Enables HTTP session replication for the selected failover group.
mac address	Specifies virtual MAC addresses for a physical interface.
interface-policy	Sets the policy for failover due to interface failures.

This information should be configured in the primary unit only.

Context: Allocate Interfaces and Assign a Failover Group Number
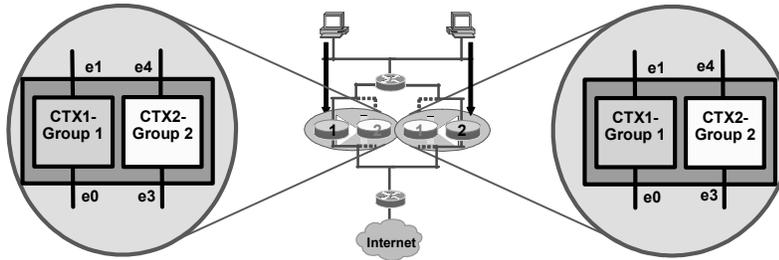
- **Associate interfaces and a group to a context**

```
fw2(config)# context ctx1
fw2(config-ctx)# allocate-interface ethernet0
fw2(config-ctx)# allocate-interface ethernet1
fw2(config-ctx)# config-url flash:/ctx1.cfg
fw2(config-ctx)# join-failover-group 1
fw2(config)# context ctx2
fw2(config-ctx)# allocate-interface ethernet3
fw2(config-ctx)# allocate-interface ethernet4
fw2(config-ctx)# config-url flash:/ctx2.cfg
fw2(config-ctx)# join-failover-group 2
```

SNPA v4.0—16-37

Once the failover groups are defined, the administrator can join contexts to failover groups and allocate context interfaces in the system configuration. In the example in the figure, the administrator allocated security appliance interfaces e0 and e1 to context CTX1, and interfaces e3 and e4 to context CTX2. The administrator joined CTX1 to failover Group 1 and CTX2 to failover Group 2. This information should be configured in the primary unit only.

The syntax for the join-failover-group command is as follows:

join-failover-group *group_num*

Context: Configure Interfaces
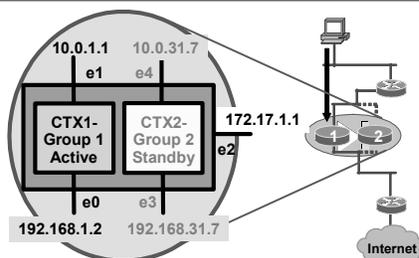
Context 1
- **Interface e0**
  - **IP address 192.168.1.2**
  - **Standby 192.168.1.7**
- **Interface e1**
  - **IP Address 10.0.1.1**
  - **Standby 10.0.1.7**

Context 2
- **Interface e3**
  - **IP address 192.168.31.7**
  - **Standby 192.168.31.7**
- **Interface e4**
  - **IP address 10.0.31.7**
  - **Standby 10.0.31.7**

```
fw2(config)# changeto context ctx1
fw2/ctx1(config)# interface ethernet0
fw2/ctx1(config-if)# ip address 192.168.1.2 255.255.255.0 standby 192.168.1.7
fw2/ctx1(config-if)# nameif outside
fw2/ctx1(config-if)# exit
fw2/ctx1(config)# interface ethernet1
fw2/ctx1(config-if)# ip address 10.0.1.1 255.255.255.0 standby 10.0.1.7
fw2/ctx1(config-if)# nameif inside
fw2/ctx1(config-if)# exit
```

SNPA v4.0—16-38

After the security appliance interfaces are allocated to each context, you can change to each active context to assign IP and standby addresses to each of the allocated interfaces. You must enter the configuration of an individual context on the unit where the context is active. If the configuration is submitted to a standby context, a warning is given. In the example in the figure, the administrator changed to context CTX1 and assigned IP address 192.168.1.2 and standby address 192.168.1.7 to interface e0. When the interface is active, the interface IP address is 192.168.1.2. When the interface is in standby or failed, the interface IP address is 192.168.1.7. Once you finish the configuration in the security appliance, enter the failover command in both security appliances to enable active/active failover. Configure this information in the active context only.

Show Failover: Part 1

Primary

10.0.1.1   10.0.31.7
e1   e4

CTX1-Group 1 Active   CTX2-Group 2 Standby   172.17.2.1
e2

e0   e3
192.168.1.2   192.168.31.7

Internet

10.0.1.7   10.0.31.1
e1   e4

172.17.2.7   CTX1-Group 1 Standby   CTX2-Group 2 Active
e2

e0   e3
192.168.1.7   192.168.31.1
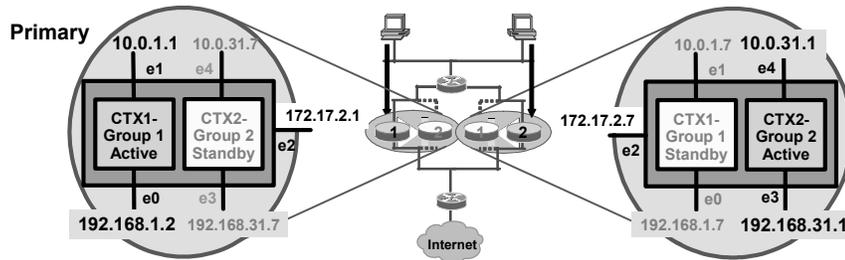
```
fx2# show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: lanfail Ethernet2 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
Group 1 last failover at: 15:54:49 UTC Dec 14 2004
Group 2 last failover at: 15:55:00 UTC Dec 14 2004
```

SNPA v4.0—16-39

The **show failover** command statistics can be broken down into three logical sections: failover LAN, primary unit, and secondary unit. The example in the figure displays the failover LAN statistics. The table shows some of the available failover statistics.

Statistic	Description
Failover	■ On ■ Off
Failover Unit	Primary or Secondary.
Failover LAN Interface	Displays the logical and physical name of the failover link.
Unit Poll Frequency	Displays the number of seconds between hello messages sent to the peer unit and the number of seconds during which the unit must receive a hello message on the failover link before declaring the peer failed.
Interface Poll Frequency	*n* seconds. The number of seconds you set with the **failover polltime interface** command. The default is 15 seconds.
Interface Policy	Displays the number or percentage of interfaces that must fail before triggering failover.
Monitored Interfaces	Displays the number of interfaces monitored, out of the maximum possible.
Group 1 Last Failover at: Group 2 Last Failover at:	The date and time of the last failover for each group in the following form: *hh*:*mm*:*ss* **UTC** *DayName Month Day yyyy* UTC (Coordinated Universal Time) is equivalent to GMT (Greenwich Mean Time).
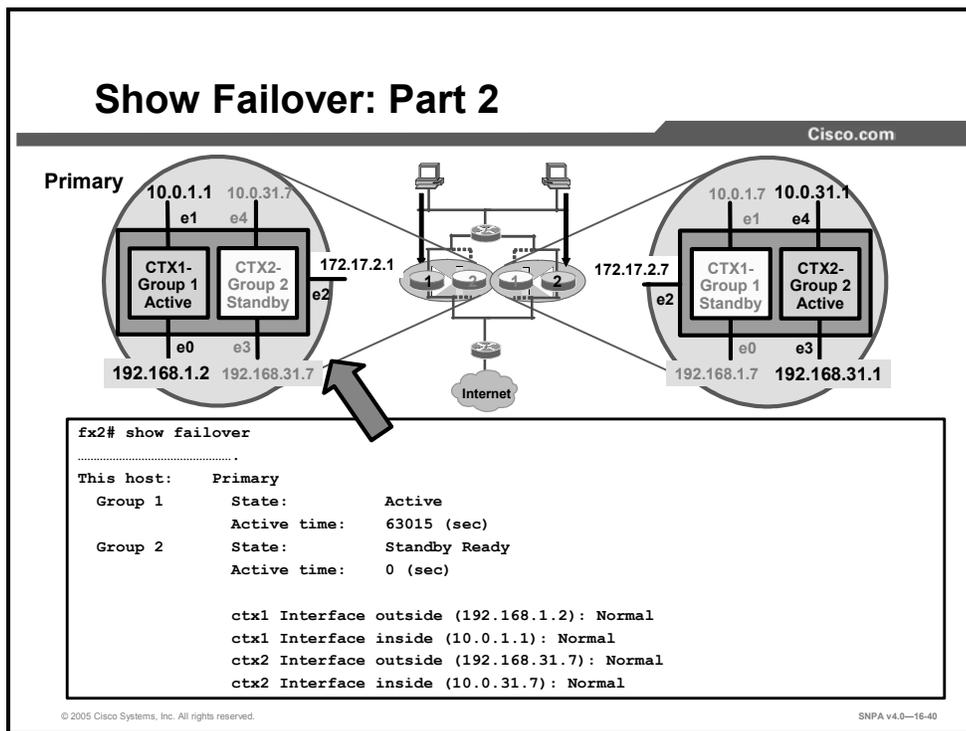
The second logical section of the **show failover** command shows statistics of the primary failover unit. In the primary security appliance, the command displays the state of each group, such as active, standby, or failed. The command also details the interface information by context; for example: `ctx1 Interface inside (10.0.1.1): Normal` The table shows some of the available failover statistics.

Statistic	Description
This host: Other host:	Shows the information for each host.
Role	Primary or Secondary
System State	■ Active or Standby Ready ■ Active Time in seconds
Group 1 State Group 2 State	■ Active or Standby Ready ■ Active Time in seconds
context Interface *name* (*n.n.n.n*):	For each interface, the display shows the IP address currently being used on each unit, as well as one of the following conditions: ■ Failed—The interface has failed. ■ No link—The interface line protocol is down. ■ Normal—The interface is working correctly. ■ Link Down—The interface has been administratively shut down. ■ Unknown—The security appliance cannot determine the status of the interface. ■ Waiting—Monitoring of the network interface on the other unit has not yet started.

Show Failover: Part 3


```
fx2# show failover
.............................. . .
Other host:   Secondary
  Group 1      State:          Standby
               Active time:    0 (sec)
  Group 2      State:          Active
               Active time:    61815 (sec)

               ctx1 Interface outside (192.168.1.7): Normal
               ctx1 Interface inside (10.0.1.7): Normal
               ctx2 Interface outside (192.168.31.1): Normal
               ctx2 Interface inside (10.0.31.1): Normal
```

The third logical section of the **show failover** command shows statistics of the peer failover unit, the secondary unit. This section of the command displays the state of the peer, such as active, standby, or failed. The command also details the interface information by context, for example: `ctx2 Interface outside (192.168.31.1): Normal` The table shows some of the available failover statistics.

Statistic	Description
This host: Other host:	Shows the information for each host.
Role	Primary or Secondary
System State	■ Active or Standby Ready ■ Active Time in seconds
Group 1 State Group 2 State	■ Active or Standby Ready ■ Active Time in seconds
context Interface *name* (*n.n.n.n*):	■ For each interface, the display shows the IP address currently being used on each unit, as well as one of the following conditions: ■ Failed—The interface has failed. ■ No link—The interface line protocol is down. ■ Normal—The interface is working correctly. ■ Link Down—The interface has been administratively shut down. ■ Unknown—The security appliance cannot determine the status of the interface. ■ Waiting—Monitoring of the network interface on the other unit has not yet started.

Show Failover Group

```
fx2# show failover group 1

  Last Failover at: 15:54:49 UTC Dec 14 2004

  This host:      Primary
                  State:          Active
                  Active time:    61920 (sec)

                  ctx1 Interface outside (192.168.1.2): Normal
                  ctx1 Interface inside (10.0.1.1): Normal
                  ctx2 Interface outside (192.168.31.7): Normal
                  ctx2 Interface inside (10.0.31.7): Normal
```

The administrator is also able to view the statistics for a specific failover group via the **show failover group** command. With the **show failover group** command, the administrator can display the state of the failover group and the interfaces on the unit.

Switch a Failover State

Cisco.com

Primary

e1   e3

CTX1-   CTX2-
Group 1   Group 2   172.17.2.1
Active   Standby
                      e4

e0   e2

Internet
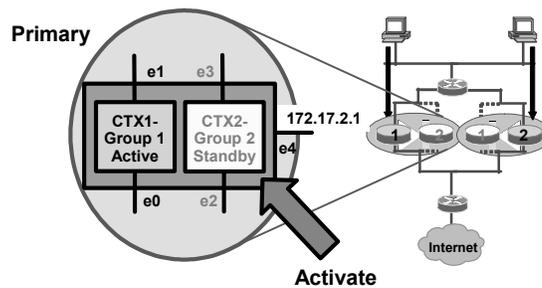
Activate

- **Activate a group, or unit.**
  - **Change CTX2 from standby to active.**

```
fw2(config)# failover active group 2
```

SNPA v4.0—16-43

You can activate a unit by using the **failover active** command. You can activate a group by adding the **group** keyword to the command string, as in the **failover active group** command. In the example in the figure, the administrator wants to activate standby CTX2 in the primary unit. To activate CTX2, enter the **failover active group 2** command in the primary unit. To de-activate a context, you can use the **no** version of the command. For example, to deactivate CTX1 in the figure, the administrator enters **no failover active group 1** command to force the switchover.

In active/active failover, failover can be triggered at the unit level if one of the following events occurs:

- The unit has a hardware failure.

- The unit has a power failure.

- The unit has a software failure.

- The **no failover active** command is entered in the system execution space.

Failover is triggered at the failover group level when one of the following events occurs:

- Too many monitored interfaces in the group fail.

- The **no failover active group group_id** command is entered.

Configure the failover threshold for each failover group by specifying the number or percentage of interfaces within the failover group that must fail before the group fails. Because a failover group can contain multiple contexts, and each context can contain multiple interfaces, it is possible for all interfaces in a single context to fail without causing the associated failover group to fail.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

- **With active/standby failover, only one security appliance actively processes user traffic while the other unit acts as a hot standby, and is prepared to take over if the active unit fails.**

- **With active/active failover, both units can actively process firewall traffic while at the same time serving as a back up for their peer unit.**

- **With stateful failover, connection status is tracked and relayed between security appliances. During stateful failover, connections remain active. With stateful failover disabled, connections are dropped.**

- **The configuration of the primary security appliance is replicated to the secondary security appliance during configuration replication.**

SNPA v4.0—16-44

Lesson 17

Cisco Security Appliance Device Manager

Overview

This lesson introduces the learner to the Cisco Adaptive Security Device Manager (ASDM), and describes how to install, configure, and monitor a security appliance with the ASDM.

Objectives

Upon completing this lesson and corresponding lab, you will be able to configure and monitor security appliances with ASDM. This ability includes being able to meet these objectives:

- Describe ASDM and its capabilities
- Explain ASDM hardware and software requirements
- Prepare the security appliance to use ASDM
- Navigate ASDM configuration windows
- Configure inside-to-outside access through the Cisco PIX Firewall Security Appliance using ASDM
- Configure outside-to-inside access through the Cisco PIX Firewall Security Appliance using ASDM
- Create site-to-site VPNs using ASDM VPN wizard
- Create remote access VPNs using ASDM VPN wizard

ASDM Overview and Operating Requirements

This topic provides an overview of the ASDM and its operating requirements.
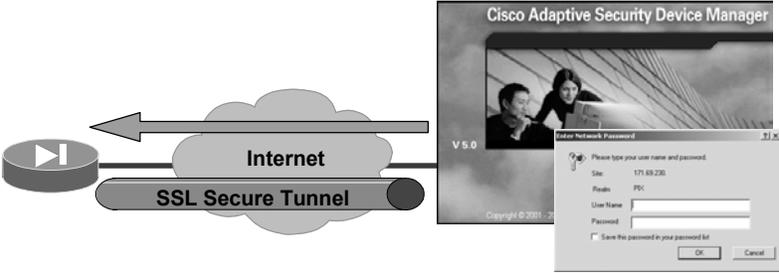
ASDM is a browser-based configuration tool designed to help the administrator set up, configure, and monitor a Cisco PIX Firewall and Adaptive Security Algorithm (ASA) Security Appliance graphically, without requiring an extensive knowledge of the security appliance command-line interface (CLI).

ASDM monitors and configures a single security appliance. You can use ASDM to create a new configuration, or to monitor and maintain current security appliances. You can point the browser to more than one security appliance and administer several security appliances from a single workstation.

ASDM Features

- **Runs on a variety of platforms**
- **Implemented in Java to provide robust, real-time monitoring**
- **Works with SSL to ensure secure communication with the PIX Firewall Security Appliance**
- **Comes preloaded in Flash memory on new PIX and ASA Security Appliances running versions 7.0**
- **ASDM sessions**
  - **5 ASDM sessions per unit (single mode) or context (multiple mode)**
  - **32 sessions per unit in multiple mode**
- **Operates on PIX 515/515E, 525, 535***
  - **Minimum software PIX Firewall version 7.0**
- **Operates on Cisco ASA 5510, 5520, and 5540**
  - **Minimum software ASA version 7.0**

* ASDM Version 5.0 is not supported on PIX Firewall 501 or 506.

SNPA v4.0—17-4

ASDM is secure, versatile, and easy to use. It manages Cisco PIX Firewall 500 Series and Cisco ASA 5500 Series security appliances and runs on a variety of platforms.

ASDM enables the administrator to securely configure and monitor a security appliance remotely. Its ability to work with the Secure Socket Layer (SSL) protocol ensures that communication with the security appliance is secure, and because it is implemented in Java, it is able to provide robust, real-time monitoring. ASDM Version 5.0 enables up to five ASDM sessions per unit in single mode or per context in multiple mode for each security appliance. In multiple mode, ASDM supports up to a total of 32 sessions per security appliance.

ASDM works with PIX Firewall and ASA Security Appliance Software Version 7.0 and comes preloaded into Flash memory on new security appliances running Software Versions 7.0. If you are upgrading from a prerelease Version 7.0 of the security appliance, the Flash memory on the security appliance is reformatted and the existing Cisco PIX Device Manager (PDM) image is not saved. You can download ASDM from Cisco and copy it to the security appliance via TFTP. In order to use ASDM, the security appliance must be running, at a minimum, PIX Firewall or ASA Software Version 7.0. ASDM runs on Windows, Sun Solaris, and Linux platforms and requires no complex software installations.

ASDM Security Appliance Requirements

A security appliance must meet the following requirements to run ASDM:

- **Security appliance software version compatible with the ASDM software version you plan to use***
- **Hardware model compatible with the ASDM software version you plan to use**
- **Activation key that enables DES or 3DES**
- **Supported Java plug-in**

* ASDM Version 5 requires Security Appliance Software Version 7.0 and does not run with earlier security appliance versions.

SNPA v4.0—17-5

A security appliance must meet the following requirements to run ASDM:

- You must have an activation key that enables Data Encryption Standard (DES) or the more secure Triple Data Encryption Standard (3DES), which ASDM requires for support of the SSL protocol. If your security appliance is not enabled for DES, you need a new security appliance activation key.

- ASDM supports Java plug-in 1.4.2 or 1.5.0. Native Internet Explorer Java Virtual Machine (JVM) may not be used.

- Verify that your security appliance meets all requirements listed in the release notes for the security appliance software version you are using.

- Verify that your security appliance hardware model, software version, and Device Manager version are compatible. Refer to the table below to ensure compatibility.

DM Version	Security Appliance SW Version	Security Appliance Model
PDM 1.0	6.0 or 6.1	506, 515, 520, 525, 535
PDM 1.1	6.0 or 6.1	506, 515, 520, 525, 535
PDM 2.0	6.2	501,506/506E, 515/515E, 520, 525, 535
PDM 2.1	6.2	501, 506/506E, 515/515E, 520, 525, 535
PDM 3.0	6.3	501, 506/506E, 515/515E, 520, 525, 535
ASDM 5.0	**7.0**	515/515E, 525, 535, 5510, 5520, 5540

ASDM Browser Requirements

To access ASDM from a browser, you must meet the following requirements:

- **JavaScript and Java must be enabled.**
- **Browser support for SSL must be enabled.**
- **Popup blockers may prevent ASDM from starting.**

SNPA v4.0—17-6

To access ASDM from a browser, you must meet the following requirements:

- JavaScript and Java must be enabled. If these are not enabled, ASDM helps you to enable them. Java plug-in Version 1.4.2 or 1.5.0 is supported. To check which version you have, launch ASDM. In the main ASDM menu, click **Help > About Cisco ASDM 5.0 for PIX**. When the About Cisco ASDM 5.0 for PIX window opens, it displays the browser specifications in a table, including the Java version. If you have an older Java version, you can download the supported Java plug-in version from Microsoft.

- Browser support for SSL must be enabled. The supported versions of Internet Explorer and Netscape Navigator support SSL without requiring additional configuration.

- Popup blockers may prevent ASDM from starting. If ASDM does not start, you should disable popup blocking.

Supported Platforms

SNPA v4.0—17-7

- **Windows**
- **Sun Solaris**
- **Linux**
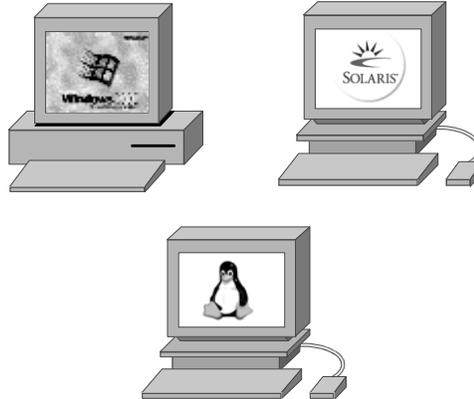
ASDM can operate in browsers running on Windows, SUN Solaris, or Linux operating systems. The requirements for each operating system are as follows:

Windows Requirements

The following requirements apply to the use of ASDM with Windows:

- Windows 2000 (Service Pack 3) or Windows XP operating systems
- Supported browsers are Internet Explorer 6.0 with Java plug-in 1.4.2 or 1.5.0, and Netscape Communicator 7.1 or 7.2, with Java plug-in 1.4.2 or 1.5.0
- Any Pentium or Pentium-compatible processor running at 450 MHz or higher
- At least 256 MB of RAM
- A 1024 x 768 pixel display with at least 256 colors
- ASDM does not support use on Windows 3.1, 95, 98, ME, or NT4

SUN Solaris Requirements

The following requirements apply to the use of ASDM with Sun Solaris/SPARC:

- Sun Solaris 2.8 or 2.9 running CDE window manager
- SPARC microprocessor
- Mozilla 1.7.3 with Java plug-in 1.4.2 or 1.5.0
- At least 256 MB of RAM
- A 1024 x 768 pixel display with at least 256 colors

Linux Requirements

The following requirements apply to the use of ASDM with Linux:

- Red Hat Linux 9.0 or Red Hat Linux WS, Version 3 running the GNOME or KDE

- Mozilla 1.7.3 with Java Plug-in 1.4.2 or 1.5.0

- At least 256 MB of RAM

- A 1024 x 768 pixel display with at least 256 colors

General Guidelines

The following are a few general guidelines for workstations running ASDM:

- You can run several ASDM sessions on a single workstation. The maximum number of ASDM sessions that you can run varies depending on the workstation resources, such as memory, CPU speed, and browser type.

- The time required to download the ASDM applet can be greatly affected by the speed of the link between your workstation and the PIX Firewall Security appliance. A minimum 56-kbps link speed is required; however, 384 kbps or higher is recommended. After the ASDM applet is loaded on your workstation, the link speed impact on ASDM operation is negligible.

If your workstation resources are running low, you should close and reopen your browser before launching ASDM.

Running ASDM
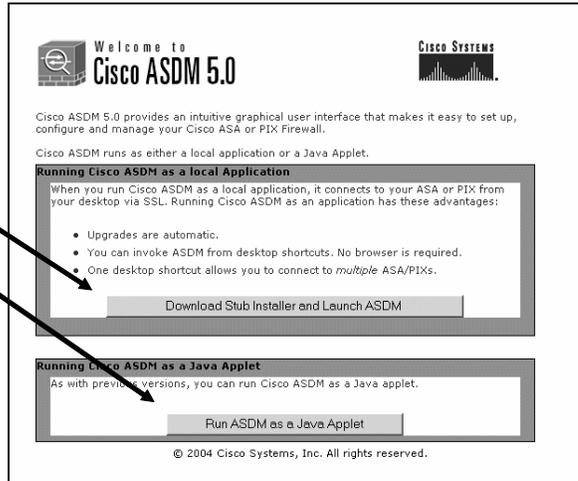
There are two options for running ASDM. When you first access ASDM via a browser, you are presented with the screen in the figure. You can choose to download the ASDM application to a PC and run it locally, or run ASDM as a Java applet via the browser. With the local ASDM application option, you can invoke ASDM from a desktop shortcut, and no browser is required. Local installation support is only provided for Windows platforms. The other option is to run ASDM as a Java applet via a browser. Once the Java applet choice is selected, a Java applet is loaded to the PC from the security appliance.

Prepare for ASDM

This topic describes the configuration of the security appliance to enable the use of ASDM.

Configure the Security Appliance to Use ASDM

Cisco.com

- **Before you can use ASDM, you need to enter the following information on the security appliance via a console terminal:**
  - **Time**
  - **Inside IP address**
  - **Inside network mask**
  - **Host name**
  - **Domain name**
  - **Enable the HTTP server on the security appliance**
  - **IP addresses of hosts authorized to access HTTP server**

© 2005 Cisco Systems, Inc. All rights reserved.   SNPA v4.0—17-10

You can either preconfigure a new security appliance through the interactive prompts, which appear after the security appliance boots, or enter the commands shown below each information item. The security appliance must be configured with the following information before you can use ASDM:

■ **Time:** Set the security appliance clock to Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT). For example, if you are in the Pacific Daylight Savings time zone, set the clock eight hours ahead of your local time to set the clock to UTC. Enter the year, month, day, and time. Enter the UTC time in 24-hour time as hour:minutes:seconds (*hh:mm:ss*). The command syntax for setting the clock is as follows:

clock set *hh:mm:ss day month year*

■ **Inside IP address:** Specify the IP address of the inside interface of the security appliance. Ensure that this IP address is unique on the network and not used by any other computer or network device, such as a router. The command syntax for setting an inside IP address is as follows:

ip address *ip_address* [netmask]

■ **Hostname:** Specify up to 16 characters as a name for the security appliance. The command syntax for setting a hostname is as follows:

hostname *newname*

■ **Domain name:** Specify the domain name for the security appliance. The command syntax for enabling the domain name is as follows:

domain-name *name*

- **IP address of the host running ASDM:** Specify the IP address of the workstation that will access ASDM from its browser. The command syntax for granting permission for a host to connect to the security appliance with SSL is as follows:

  http *ip_address* [netmask] [if_name]

- **HTTP server:** Enable the HTTP server on the security appliance. The command syntax for setting a hostname is as follows:

  http server enable command

Setup Dialog

```
Pre-configure Firewall now through interactive prompts [yes]? <Enter>
Security Appliance Mode [routed]:
Enable Password [<use current password>]: cisco123
Allow password recovery [yes] ?
Clock (UTC)
  Year [2004]: <Enter>
  Month [Jul]: <Enter>
  Day [29]: <Enter>
  Time [10:21:49]: <Enter>
Inside IP address: 10.0.1.1
Inside network mask: 255.255.255.0
Host name: pix1
Domain name: ciscopix.com
IP address of host running PIX Device Manager: 10.0.1.11
Use this configuration and write to flash? Y
```

SNPA v4.0—17-11

A security appliance starts as an interactive setup dialog to enable you to perform the initial configuration required to use ASDM. You can also access the setup dialog by entering **setup** at the configuration mode prompt.

The dialog asks for several responses, including the inside IP address, network mask, host name, domain name, and ASDM host. The host name and domain name are used to generate the default certificate for the SSL connection.

The example in the figure shows how to respond to the **setup** command prompts. Pressing the **Enter** key instead of entering a value at the prompt accepts the default value within the brackets. You must fill in any fields that show no default values, and change default values as necessary. After the configuration is written to Flash memory, the security appliance is ready to start ASDM.

Note	The clock must be set for ASDM to generate a valid certification. Set the security appliance clock to UTC (also known as GMT).

The prompts in the setup dialog are as follows:

- **Security Appliance Mode [routed]:** Enables you to specify the security appliance mode, routed or transparent.

- **Enable Password:** Enables you to specify an enable password for this security appliance.

- **Clock (UTC):** Enables you to set the security appliance clock to UTC (also known as GMT).

- **Year [*system year*]:** Enables you to specify the current year, or return to the default year stored in the host computer.

- **Month [*system month*]:** Enables you to specify the current month, or return to the default month stored in the host computer.

- **Day [*system day*]:** Enables you to specify the current day, or return to the default day stored in the host computer.

- **Time [*system time*]:** Enables you to specify the current time in hh:mm:ss format, or return to the default time stored in the host computer.

- **Inside IP address:** The network interface IP address of the security appliance.

- **Inside network mask:** A network mask that applies to the inside IP address.

- **Host name:** The hostname you want to display in the security appliance command-line prompt.

- **Domain name:** The Domain Name System (DNS) domain name of the network on which the security appliance runs (for example, cisco.com).

- **IP address of host running ASDM:** IP address on which ASDM connects to the security appliance.

- **Use this configuration and write to flash?:** Enables you to store the new configuration to Flash memory. It is the same as the **write memory** command. If the answer is yes, the inside interface is enabled and the requested configuration is written to Flash memory. If the user answers anything else, the setup dialog repeats using the values already entered as the defaults for the questions.

Navigating ASDM Configuration Windows

This topic describes the layout of the ASDM configuration windows.
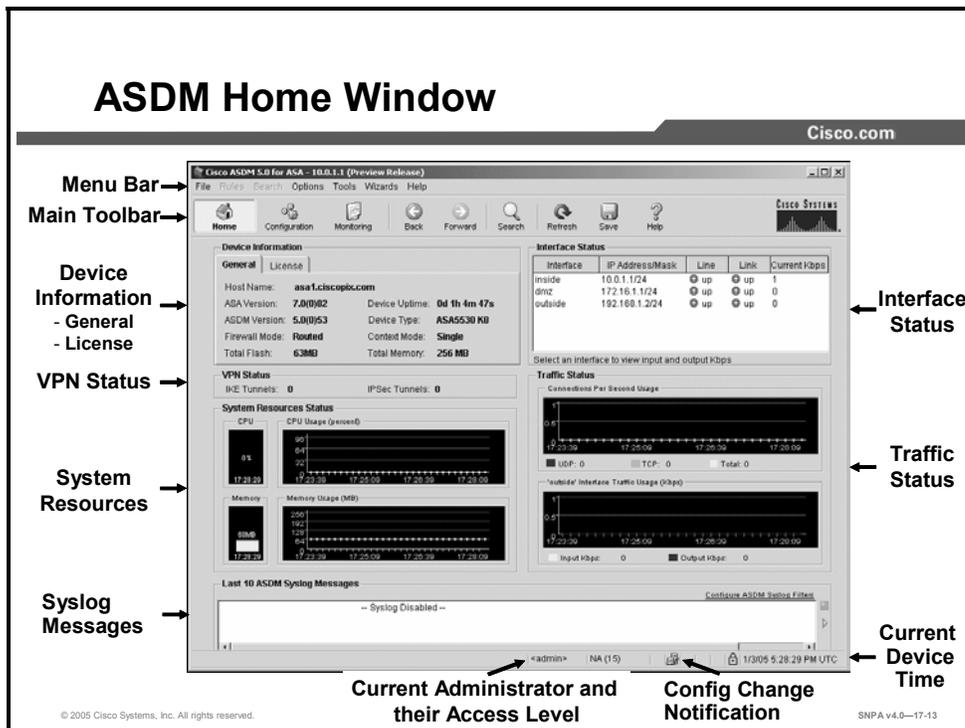
The ASDM Home window enables you to view important information about the security appliance, such as the status of the interfaces, the version running, licensing information, and performance details. Many of the details available on the ASDM Home window are available elsewhere in ASDM, but the Home window provides a useful and quick way to see how the security appliance is running. All information on the Home window is updated every ten seconds, except for the Device Information. You can access the Home window any time by clicking the Home button on the main toolbar.

The following sections are included in the ASDM Home window:

■ **Menu Bar:** Provides quick access to files, tools, options, wizards, and help.

■ **Main Toolbar:** Provides quick access to the Home window, configuration windows, ASDM monitoring, search, and context-sensitive help. You can also save the running configuration to Flash memory by clicking the **Save** button, or reload the running configuration from Flash by clicking the **Refresh** button.

■ **Device Information group box:** Displays security appliance information in two tabs, general and license. The general tab displays security appliance hardware and software information. The license tab displays the level of support for licensed features on a security appliance.

■ **System Resources Status group box:** Displays CPU and memory usage.

■ **Interface Status group box:** Displays the interface, IP address and mask, and link status.

- **Traffic Status group box:** Displays the number of TCP and UDP connections that occur each second. Their sum is displayed as the total number of connections. The Interface Traffic Usage area displays the traffic going through the named interface in kilobits per second.

- **Last 10 ASDM Syslog Messages group box:** Displays the last ten system messages generated by the security appliance.

Startup Wizard

SNPA v4.0—17-14
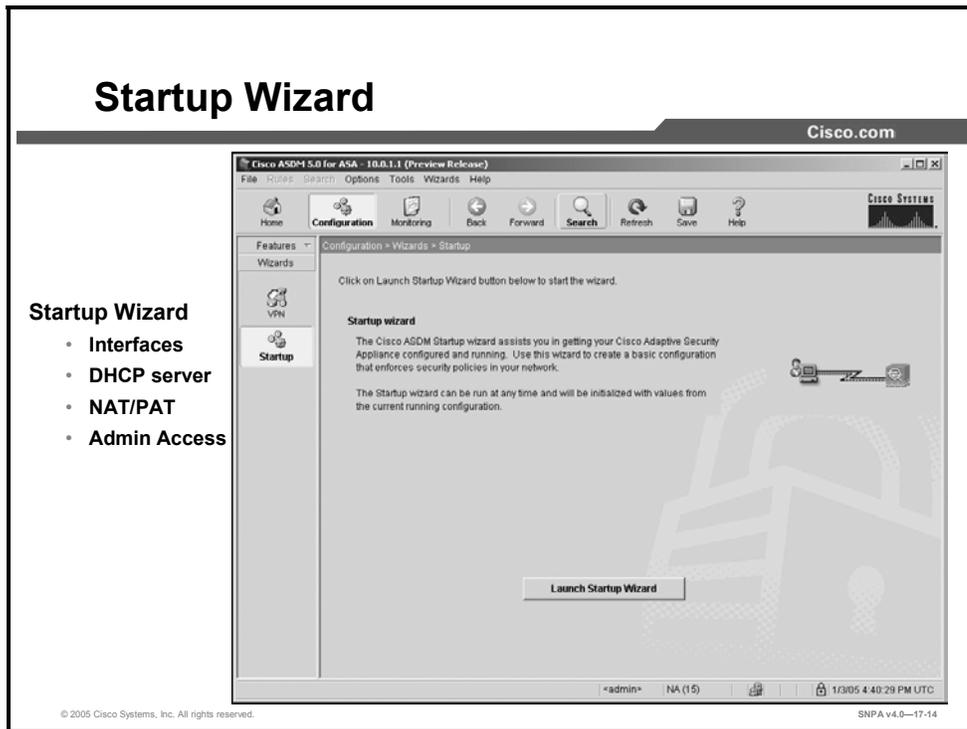
The ASDM Startup Wizard is an easy way to begin the process of configuring the security appliance. The wizard steps you through such tasks as the following:

- Enabling the security appliance interfaces

- Assigning IP addresses to the interfaces

- Configuring a host name and password

- Configuring Network Address Translation (NAT) and Port Address Translation (PAT)

- Configuring the Dynamic Host Configuration Protocol (DHCP) server

After stepping through the wizard, you can use **Configuration > Features** to view, add, and modify security appliance features.

VPN Wizard

VPN Wizard
- **Site-to-site**
- **Remote Access**

* Use Configuration > VPN to edit VPN connections

SNPA v4.0—17-15

The virtual private network (VPN) wizard enables you to configure basic site-to-site and remote access VPN connections. Click the **Launch VPN Wizard** button to step through the configuration tasks necessary to establish a basic remote access or site-to-site VPN tunnel. There are two VPN wizard configuration options, as described here:

- **Site-to-Site Option:** Use **Site-to-Site** to create a LAN-to-LAN VPN configuration. Use between two IPSec security gateways, which can include security appliances, VPN concentrators, or other devices that support site-to-site IPSec connectivity. After you click the **Launch VPN Wizard** button , you may select this option. The VPN wizard displays a series of windows that lets them enter the attributes a site-to-site VPN requires.

- **Remote Access Option:** Use **Remote Access** to create a configuration that achieves secure remote access for VPN clients, such as mobile users. This option lets remote users securely access centralized network resources. After you click the **Launch VPN Wizard** button , you may select this option. The VPN wizard displays a series of windows that let you enter the attributes a remote access VPN requires.

Use ASDM **Configuration > Features > VPN** to view, add, and modify advanced VPN features on established VPN tunnels.

Configuration Window

Configuration:
- **Interface**
- **Security Policy**
- **NAT**
- **VPN**
- **IPS**
- **Routing**
- **Building Blocks**
- **Device Admin**
- **Properties**

SNPA v4.0—17-16

The ASDM configuration feature list consists of nine icons, which enable you to configure various aspects of the product: interfaces, a security policy, routing, NAT, VPN, device administration features, Intrusion Prevention System (IPS), and miscellaneous properties. You can also configure building blocks, including host and network identification and application inspection maps, to simplify your configuration tasks. Some features might not be available for your security appliance, depending on the mode and context.

The list of available configuration feature icons is as follows:

- **Interfaces:** The Interfaces window displays configured interfaces and subinterfaces. You can add or delete subinterfaces, and also enable communication between interfaces on the same security level.

- **Security Policy:** You can add and delete access rules; authentication, authorization, and accounting (AAA) rules; filter rules; and service policy rules.

- **NAT:** You can add, delete, and modify translation and translation exemption rules.

- **VPN:** You can create and modify site-to-site and remote access VPNs.

- **IPS** (Optional)**:** The IPS icon will not be present until the IPS software is installed and configured on the Advanced Inspection and Prevention-Security Services Module (AIP-SSM).

- **Routing:** You can configure static routes, passive RIP, Open Shortest Path First (OSPF), Internet Group Management Protocol (IGMP), and Protocol Independent Multicast (PIM).

- **Building Blocks:** You can configure an IP address for host name conversion, inspection maps, and time ranges.

- **Device Administration:** You can set basic administration parameters for the security appliance. You can also configure and administer certificates.

- **Properties:** You can customize your security appliance by configuring failover, logging, the static Address Resolution Protocol (ARP) table, and many other features.

Interfaces

- **IP Address**
- **Static**
- **DHCP**
- **VLAN**
- **Same Security Level**

SNPA v4.0—17-17

The Interfaces window displays configured interfaces and subinterfaces. You can add or delete subinterfaces, and also enable communication between interfaces on the same security level.

Security Policy

SNPA v4.0—17-18

- **Access Rules**
- **AAA Rules**
- **Filter Rules**
- **Service Policy Rules**

You can add and delete access rules, AAA rules, filter rules, and service policy rules. The available rules are as follows.

- **Access rules:** The Access Rules window shows your entire network security policy expressed in rules. When you click the **Access Rules** option, this window enables you to define access control lists (ACLs) to control the access of a specific host or network to another host or network, including the protocol or port that can be used.

- **AAA rules:** When you click the **AAA Rules** option button, you can define AAA rules. AAA tells the security appliance who the user is, what the user can do, and what the user did. You can use authentication alone, or with authorization. Authorization always requires authentication.

- **Filter rules:** The Filter Rules window provides information about the filter rules that are currently configured on the security appliance. It also provides buttons that you can use to add or modify the filter rules and to increase or decrease the amount of detail shown in the window. Filtering allows greater control over any traffic that your security policy allows to pass through the security appliance. Instead of blocking access altogether, you can remove specific undesirable objects from HTTP traffic, such as ActiveX objects or Java appendages that may pose a security risk. You can also use URL filtering to direct specific traffic to an external filtering server, such as N2H2 or Websense. These servers can block traffic to specific sites or types of sites, as specified by your security policy.

- **Service policy rules:** Some applications require special handling by the security appliance and specific application inspection engines are provided for this purpose. Applications that require special application inspection engines are those that embed IP addressing information in the user data packet, or open secondary channels on dynamically assigned ports. Application inspection is enabled by default for many protocols, and it is disabled for other protocols. In many cases, you can change the port on which the application inspection listens for traffic. Service policy rules define how specific types of application inspection are applied to different types of traffic received by the security appliance. You can apply a specific rule to an interface, or globally to every interface.

NAT

Cisco.com

- **NAT Control**
- **Translation Rules**
  - **NAT**
  - **Policy NAT**
  - **Max Conns**
  - **Embryonic Conns**
- **Translation Exemption Rules**
  - **NAT0**

SNPA v4.0—17-19
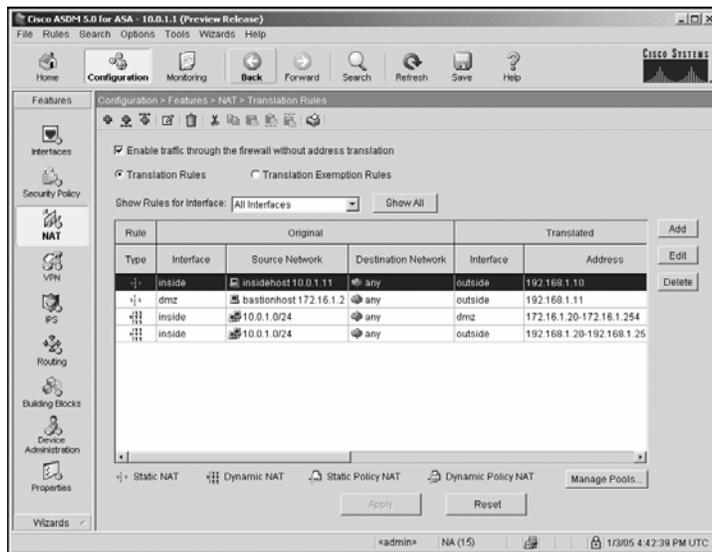
The security appliance supports both Network Address Translation (NAT) and Port Address Translation (PAT) features. NAT provides a globally unique address for each outbound host session. The PAT feature provides a single, unique global address for up to 64,000 simultaneous outbound or inbound host sessions. The global addresses used for NAT come from a pool of addresses used specifically for address translation. The unique global address that is used for PAT can either be one global address or the IP address of a given interface. The available rules are as follows:

- **Translation Rules:** Enables you to view all the address translation rules

- **Translation Exemption Rules:** Enables you to specify traffic that is exempt from being translated or encrypted

---

Note   The order in which you apply translation rules can affect the way the rules operate. ASDM lists the static translations first and then the dynamic translations. When processing NAT, the security appliance first translates the static translations in the order they are configured. You can use the **Insert Before** or **Insert After** command from the Rules menu to determine the order in which static translations are processed. Because dynamically translated rules are processed on a best-match basis, the option to insert a rule before or after a dynamic translation is disabled.

The Manage Pools button enables you to create global address pools to be used by NAT. From the Manage Pools window, you can view or delete existing global pools.

VPN

Cisco.com

Edit VPN
- **IKE**
- **IPSec**
- **IP address management**
- **VPN General**
- **WebVPN**
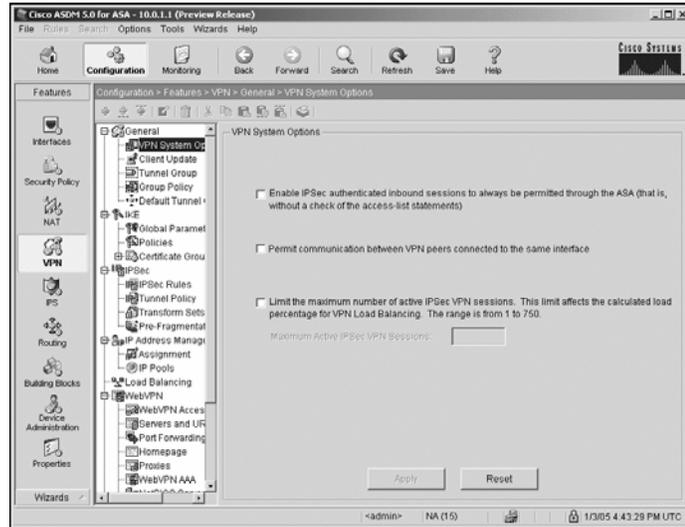
* Use Remote Access or Site-to-Site VPN Wizard for new VPN connections

SNPA v4.0—17-20

The security appliance creates a VPN by creating a secure connection across a TCP/IP network (such as the Internet). The ASDM can configure remote access, site-to-site, and WebVPN connections. WebVPN is only supported on ASA 5500 Series security appliances. You can use the VPN wizard to create site-to-site and remote access VPNs. After the VPN tunnels are configured via the wizard, the VPN feature commands enable you to add, delete, or modify VPN features on the security appliance. The major configuration topics in the IPSec menu tree are IKE, IPSec, IP address management, and WebVPN.

VPN Policy Configuration

VPN Group Policy

VPN Tunnel Group

SNPA v4.0—17-21
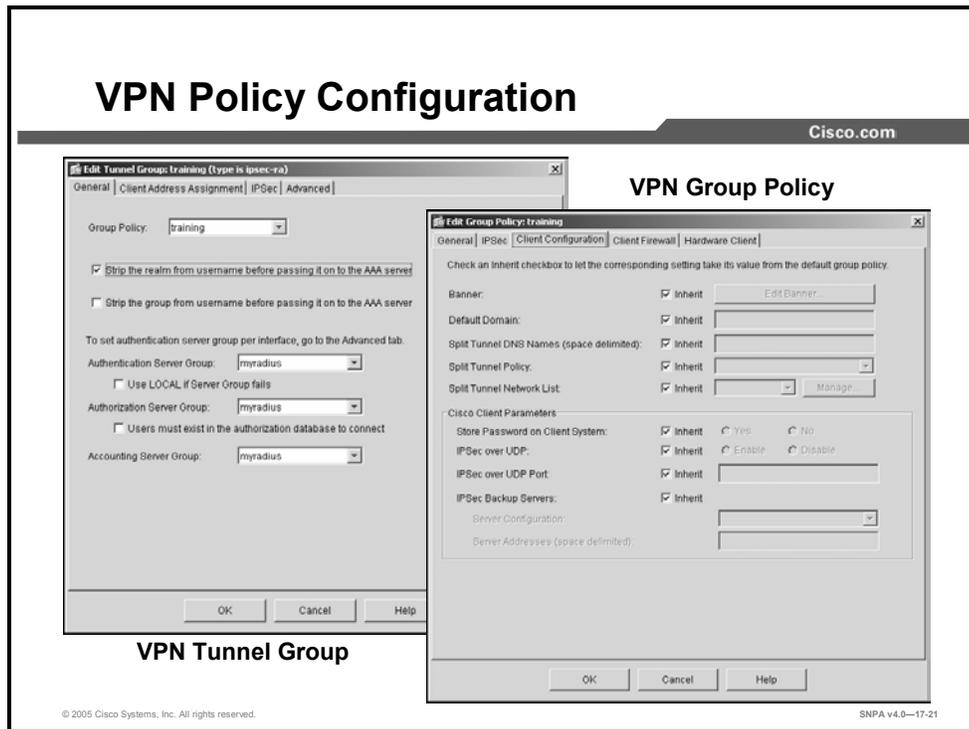
After you add a VPN tunnel via the VPN Wizard, you can return to the VPN configuration icon and configure individual VPN tunnel and group policies. Two examples of the available VPN windows are Edit Tunnel Group and Edit Group Policy. A VPN tunnel group represents a connection-specific record for IPSec connections.

The parameters in the Tunnel Group window enable you to manage VPN tunnel groups. In the Edit Tunnel Group window, you can use the following tabs to configure parameters:

■ **General:** Enables you to specify the AAA parameters

■ **Client Address Assignment:** Enables you to select the method (or methods) of address assignment

■ **IPSec:** Enables you to configure or edit IPSec-specific tunnel group parameters

■ **Advanced:** Enables you to specify interface-specific information

The Edit Group Policy window enables you to manage VPN group policies. A VPN group policy is a collection of user-oriented attributes or value pairs stored either internally on the device or externally on a Remote Authentication Dial-In User Service (RADIUS) or Lightweight Directory Access Protocol (LDAP) server.

In the Edit Group Policy window, you can configure the following parameters:

■ **General:** Protocols, filtering, connection settings, and servers

■ **IPSec:** IP Security tunneling protocol parameters and client access rules

■ **Client Configuration:** Banner, password storage, split-tunneling policy, default domain name, IPSec over UDP, backup servers

■ **Client Firewall:** VPN Client personal firewall requirements

■ **Hardware Client:** Interactive hardware client and individual user authentication; network extension mode

■ **WebVPN:** SSL VPN access (ASA Security Appliance only)

Routing
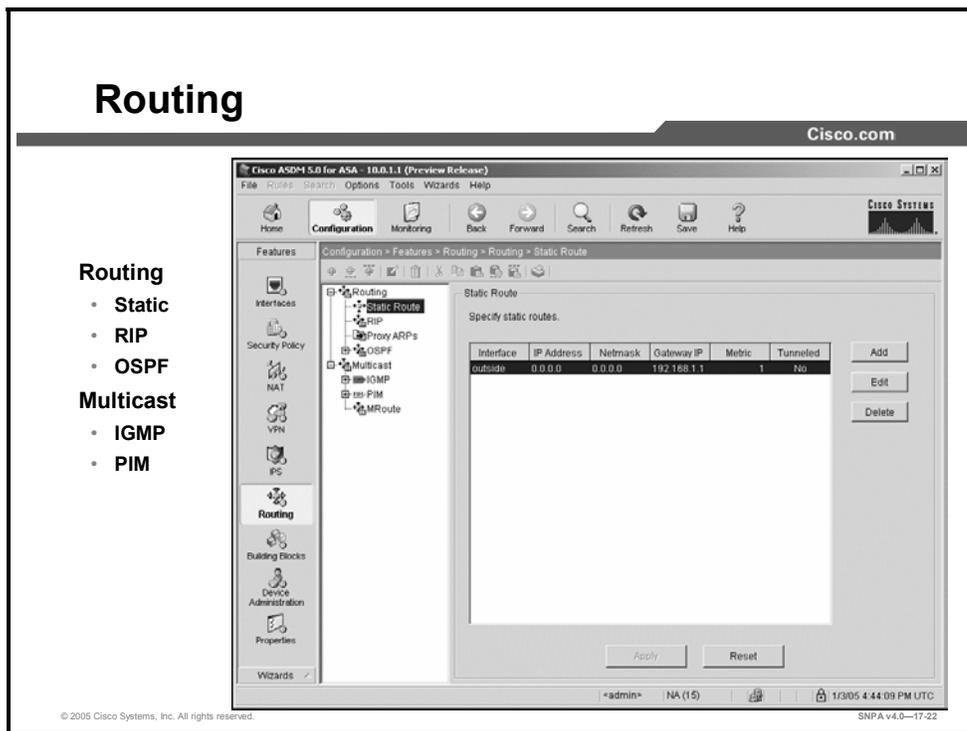
Routing
- **Static**
- **RIP**
- **OSPF**

Multicast
- **IGMP**
- **PIM**

SNPA v4.0—17-22

The Routing feature enables you to configure routing. The Routing window is subdivided into Static Route, RIP, Proxy ARPs, OSPF, IGMP, and PIM. An overview of each is as follows:

■ **Static route:** Enables you to add or modify a static route to ensure that the security appliance correctly forwards network packets destined to the host or network. You can also use a static route to override any dynamic routes that are discovered for this host or network by specifying a static route with a lower metric than the discovered dynamic routes.

■ **RIP:** Enables you to configure RIP Version 1 or RIP Version 2 on an interface. Additionally, RIP Version 2 enables you to configure Version 2 authentication parameters.

■ **Proxy ARP:** Enables you to enable or disable proxy on an interface basis.

■ **OSPF:** Enables you to configure OSPF processes, OSPF areas and networks, neighbors, filtering, redistribution, and define OSPF route summarization.

■ **Multicast:** Enables you to configure multicast routing on the security appliance. Enabling multicast routing enables IGMP and PIM on all interfaces by default. IGMP is used to learn whether members of a group are present on directly attached subnets. PIM is used to maintain forwarding tables to forward multicast datagrams.

Building Blocks

SNPA v4.0—17-23
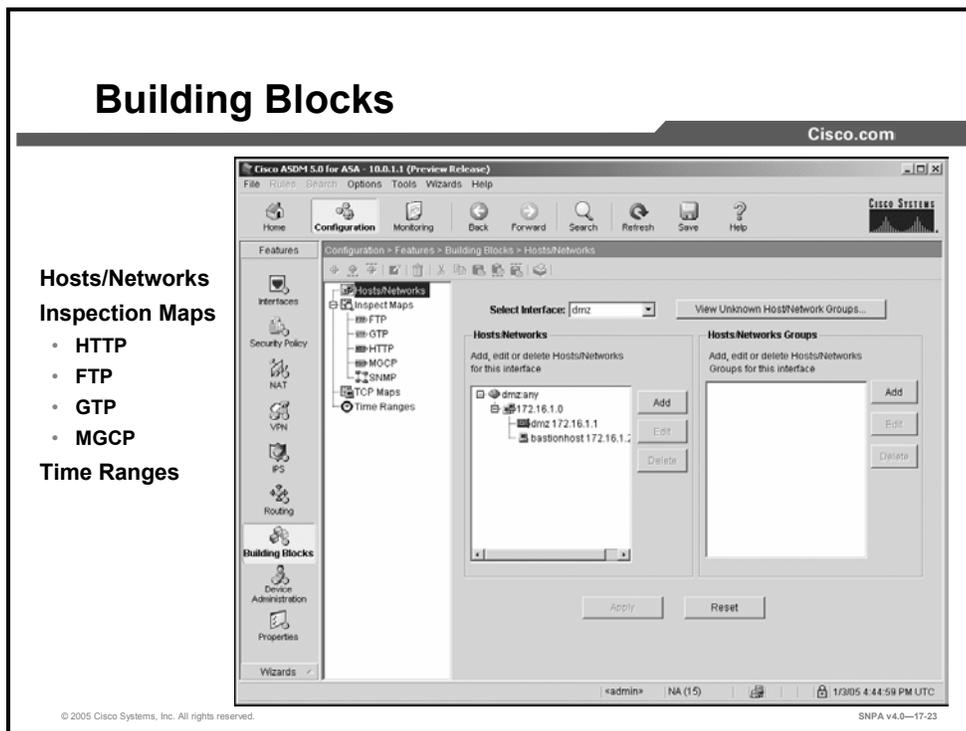
When you configure the security appliance using ASDM, you can create building blocks in advance to make configuration more streamlined. You can configure parameters as follows:

- **Hosts/Networks window:** Enables you to predefine host and network IP addresses. It also enables you to keep track of the network topology.

- **Inspection Maps:** Enables you to configure protocol inspection rules for specific protocols. The inspection maps can be later applied to a service policy. The subtopics under Inspection Maps are as follows:

  — HTTP: Enables you to change the default configuration values used for HTTP application inspection. From the HTTP panel, you can add a new HTTP map and change or delete an existing map.

  — FTP: Enables you change the default configuration values used for FTP application inspection. From the FTP panel, you can add a new FTP map and change or delete an existing map.

  — GTP: Enables you to change the default configuration values used for GTP application inspection. From the GTP panel, you can add a new GTP map and change or delete an existing map.

  — MGCP: Enables you to change the default configuration values used for MGCP application inspection. From the MGCP panel, you can add a new MGCP map and change or delete an existing map.

- **TCP Maps:** Enables you to customize inspection on TCP flows for the security appliance traffic. The TCP maps can later be applied to a service policy.

- **Time Ranges:** Enables you to define a time range that you can attach to traffic rules, or an action.

Device Administration

Administration

Certificate

- **Trustpoint**

SNPA v4.0—17-24

Under Device Administration, you can set basic parameters for the security appliance such as passwords, user accounts, banners, system access, and so on. You can also generate and manage certificates.

Properties

SNPA v4.0—17-25
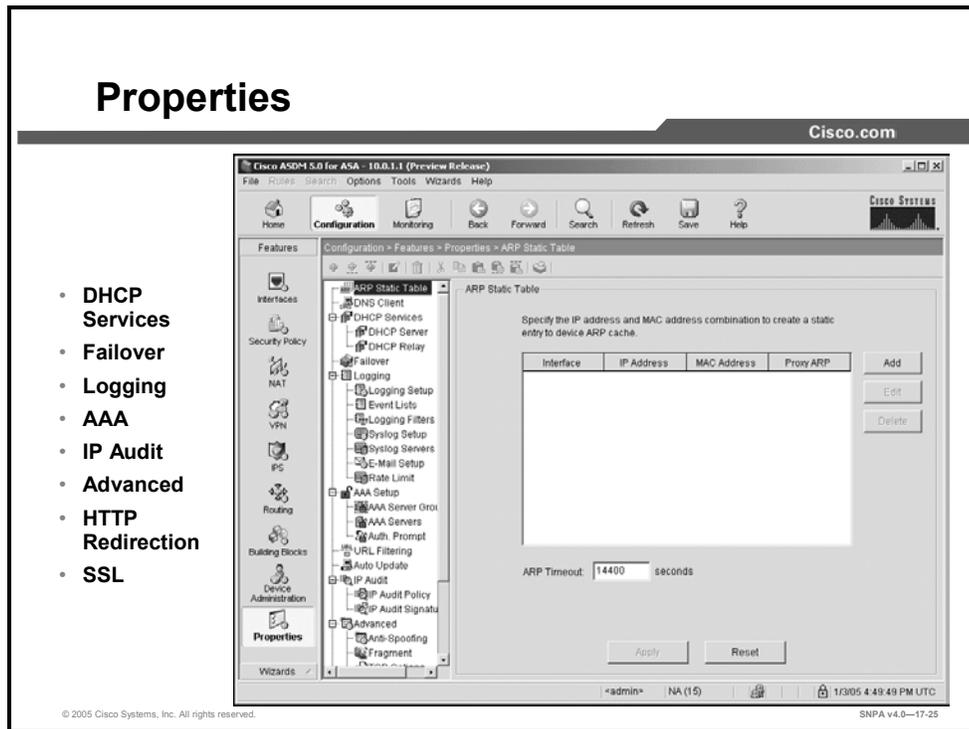
Under Properties, you can customize the security appliance by configuring failover, logging, AAA server, authentication prompts, IP audit policy and signatures, fragmentation and protocol timeouts, and so on. You can configure parameters as follows:

- **The MAC Address Table window:** Enables you to add static Media Access Control (MAC) address entries. Normally, MAC addresses are added to the MAC address table dynamically as traffic from a particular MAC address enters an interface. You can add static MAC addresses to the MAC address table if desired.

- **The DNS Client window:** Enables you to specify one or more DNS servers for the security appliance so that it can resolve server names to IP addresses.

- **A DHCP server window:** Provides network configuration parameters, such as IP addresses, to DHCP clients. The security appliance can provide DHCP server or DHCP relay services to DHCP clients attached to security appliance interfaces. The DHCP server provides network configuration parameters directly to DHCP clients. DHCP relay passes DHCP requests received on one interface to an external DHCP server located behind a different interface.

- **The Failover window:** Provides the settings for configuring failover on the security appliance.

- **The Logging window:** Enables you to enable or disable the sending of informational messages to the console, to a syslog server, or to an SNMP management station.

- **The AAA Setup windows:** Enables you to configure AAA server groups, AAA servers, and the authentication prompt.

- **The Auto Update window:** Enables the Auto Update server to push configuration information and send requests for information to the security appliance. It also enables the Auto Update server to pull configuration information by causing the security appliance to periodically poll the Auto Update server.

- **The IP audit window:** Provides basic IPS functionality. For advanced IPS functionality on supported platforms, you can install an AIP SSM.

- **Advanced window:** Enables you to configure advanced protection features, including anti-spoofing, fragment options, and connection settings.

- **The History Metrics window:** Enables you to configure the security appliance to keep a history of various statistics, which can be displayed by ASDM on any graph or table. If you do not enable history metrics, you can only monitor statistics in real time.

- **The HTTP/HTTPS window:** Provides a table that displays information on HTTP redirection and Hypertext Transfer Protocol secure (HTTPS) user certificate requirements for each interface on the security appliance.

- **The priority-queue window:** Enables you to create a priority queue for an interface before priority queuing takes effect. In priority-queue mode, you can configure the maximum number of packets allowed in the transmit queue at any given time (**tx-ring-limit** command) and the number of packets of either type (priority or best-effort) allowed to be buffered before dropping packets (**queue-limit** command).

Monitoring Button

Monitoring
- **Interfaces**
- **Routing**
- **VPN**
- **Administration**
- **Connections**
- **Logging**
- **IP Audit**

SNPA v4.0—17-26
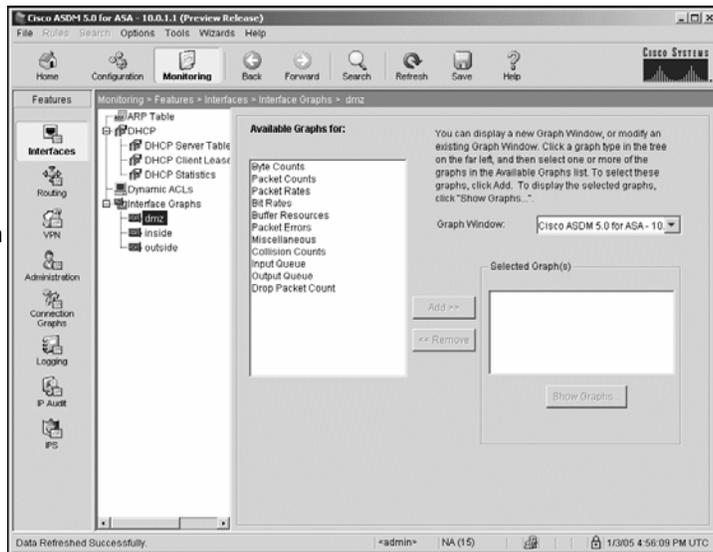
Many different items can be monitored using ASDM, including but not limited to the following:

- Interfaces
- Routing
- VPN
- Administration
- Connections
- Logging
- IP Audit

Interface Graphs Panel

The Interface Graphs panel enables you to monitor per-interface statistics, such as bit rates, for each enabled interface on the PIX Firewall.
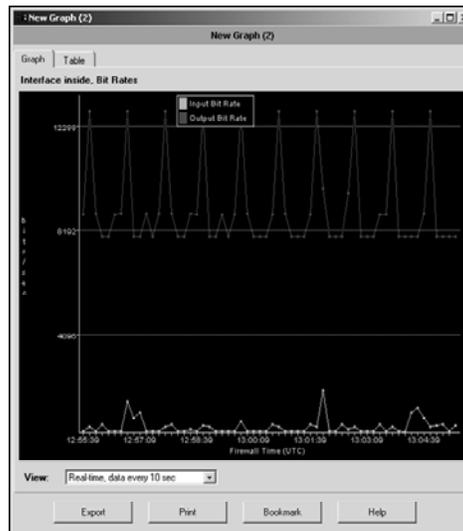
SNPA v4.0—17-27

ASDM enables you to monitor all aspects of the security appliance, including performance, statistics, and connections. You can also view the system message log buffer. For statistics shown in graph or table form, you can view the statistics for the last five minutes in real time. Enabling History Metrics enables you to view statistics graphs from the last 10 minutes, 60 minutes, 12 hours, or 5 days.

Search

SNPA v4.0—17-28
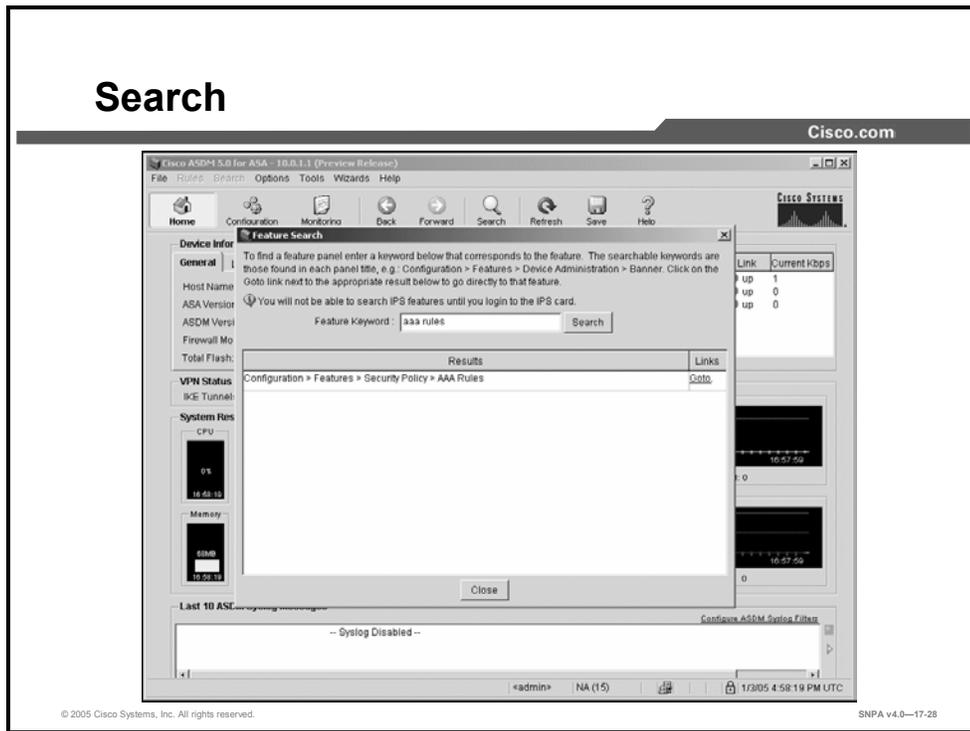
The Search enables you to find configuration windows, based on a key word. For example, you want to update the AAA rules on the security appliance, but do not remember where to find the command in ASDM. You can click on **Search** and enter "AAA rules" in the key word box. The ASDM returns a link to the AAA Rules configuration window.

Options > Preferences
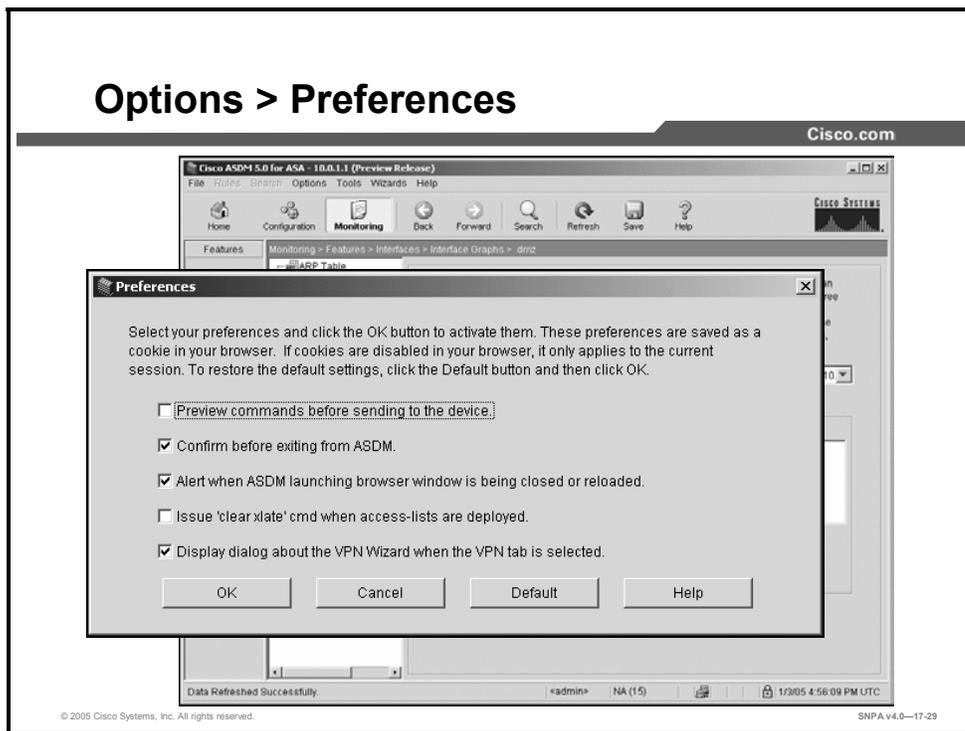
The Preferences window enables you to change the behavior of some ASDM functions between sessions. The following preferences are configurable:

- Preview commands before sending to the security appliance

- Confirm before exiting from ASDM

- Alert when ASDM launching browser window is being closed or reloaded

- Issue **clear x-late** command when access-lists are deployed

- Display dialog about the VPN Wizard when the VPN tab is selected

Tools

Tools
- **Command-Line Interface**
- **Ping**
- **Service Group**
- **File Management**
- **Upload Image from Local PC**
- **File Transfer**
- **System Reload**

SNPA v4.0—17-30
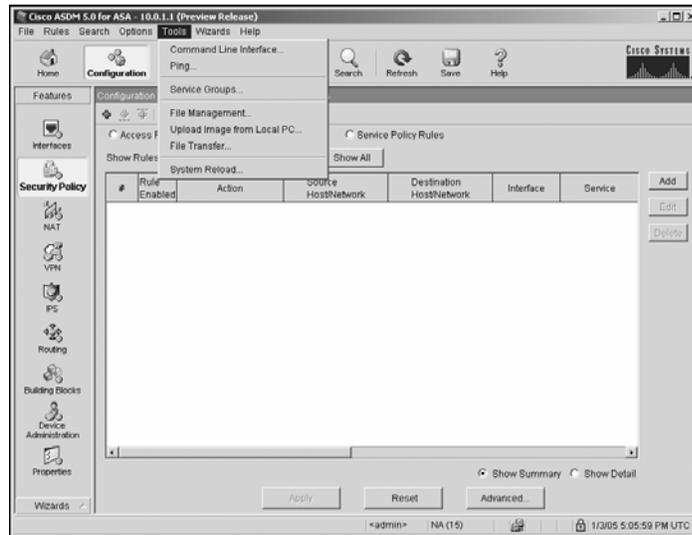
The Tools menu provides you with troubleshooting tools on ASDM. Here you can upload new software to the ASDM, upload or download files, check connectivity, check the security appliance directory files, or issue commands via the command line. You can configure parameters as follows:

- **The Command Line Interface (CLI) window:** Provides a text-based tool for sending commands to the security appliance and viewing the results.

- **The Ping window:** Provides a useful tool for verifying the configuration and operation of the security appliance and surrounding communication links, as well as basic testing of other network devices.

- **File management:** Enables you to view, move, copy, and delete files stored in Flash memory. You can also create a directory on the Flash file system.

- **Upload Image from Local PC:** Enables you to add a security appliance operating system or ASDM files to the Flash memory.

- **File Transfer:** Enables you to copy files to and from the security appliance using HTTPS, TFTP, FTP, or by browsing for a local image.

- **System Reload:** Enables you to restart the system and reload the saved configuration into memory.

Help

Help
- **Help Topics**
- **Help for Current Screen**
- **Release Notes**
- **Getting Started**
- **User Guide**
- **Glossary**
- **Legend**
- **About ASA**
- **About ASDM 5.0**

At any point, you can click the **Help** dropdown menu for help topics, help for the screen, links to release notes, links to configuration guides, description of the ASDM icons, and information about the managed security appliance, or the managing ASDM.

Online Help

SNPA v4.0—17-32

You can select the **Help > Help for Current Screen** dropdown menu to navigate through the online help to find a topic. The following menu choices are available:

- **About ASDM:** Displays information about ADSM

- **Search:** Enables you to search the help topics

- **Using Help:** Describes the best way to get the most out of online help

- **Glossary:** Lists a glossary of terms found in ASDM and networking

You can use the left-pane tabs to help you navigate the online help. These menu choices are available:

- **Contents:** Displays a table of contents

- **Screens:** Lists help files by screen name

- **Index:** Provides an index of help topics found in ASDM online help

The right pane displays the help for the topic selected in the left pane.

Navigating ASDM Multimode Windows

This topic describes managing multimode with the ASDM.

ASDM supports multiple virtual firewalls called security contexts. You can partition a single security appliance into multiple security contexts. Each context is an independent device, with its own security policy, interfaces, and administrators. Multiple contexts are similar to having multiple standalone devices. Many features are supported in multiple context mode, including routing tables, firewall features, IPS, and management.

In multiple context mode, the security appliance includes a configuration for the system and each context, as follows:

■ The system configuration identifies basic settings for the security appliance. The administrator adds and manages contexts by allocating them in the system configuration. The system configuration does not include any network interfaces or network settings for itself. The security policy, interfaces, and almost all of the security options are configured in a context.

■ The admin context is just like any other context, except that when a user logs into the admin context, that user has system administrator rights and can access the system and all other contexts. Typically, the admin context provides network access to network-wide resources, such as a syslog server or context configuration server. Many features are supported in contexts, including routing tables, firewall features, IPS, and management.

Before you can configure contexts using ASDM, make sure the security appliance is in multiple context mode. If the ASDM toolbar includes **Context** and **System** buttons, the security appliance is in multiple mode. Also, the **Home > Device Information > General** tab shows the current context mode, either multiple or single.

- To change from single mode to multiple mode, access the security appliance CLI and enter the **mode multiple** command. You can not change modes via ASDM.

- If an ASDM session is active on a security appliance when you issue a **mode multiple** command, you must restart the ASDM session.

- To change between each context configuration and the system, click **Context** or **System** on the toolbar.

- To choose between contexts, click the context name in the **Context** dropdown list.

System Configuration

SNPA v4.0—17-35

The administrator adds contexts by allocating them in the system configuration. The system configuration identifies basic settings for the security appliance. The following system information is configurable:

■ **Interface**—Displays configured interfaces and subinterfaces. Before you can configure an interface within a context, you must first allocate the context. Although the system configuration does not include any networking parameters for these interfaces, the system controls the allocation of interfaces to each context.

■ **Failover:** Includes tabs for configuring the system-level failover settings. In multiple mode, you can configure active/standby or active/active failover. In both types of failover, you need to provide system-level failover settings in the system context.

■ **Security Contexts:** Displays the configured contexts and information about each context. It also enables you to add, edit, or delete a context.

■ **Device Administration:** Sets device-level admin properties such as user accounts, the clock setting, Network Time Protocol (NTP) server settings, secure copy, FTP mode, and the default boot location for the startup configuration and software image.

The system configuration does not include any network interfaces or network settings for itself. When you need to configure network resources such as IP addresses and ACLs, you must change to a designated context.

System Monitoring

SNPA v4.0—17-36
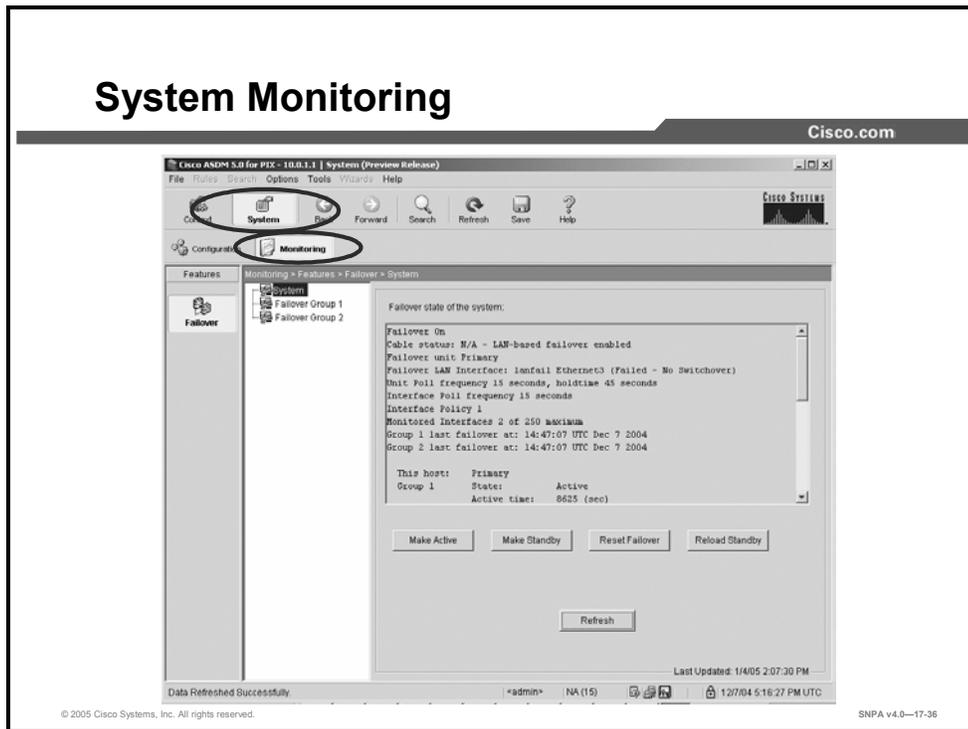
You can monitor the failover status of the system and of the individual failover groups in the system context. **Monitoring > Failover** displays the failover state of the system. You can also control the failover state of the system in the following ways:

- Toggle the active/standby state of the device.
- Toggle the active/standby state of the failover group.
- Reset a failed device.
- Reload the standby unit.

Context Configuration

SNPA v4.0—17-37

When you need to configure the network resources, select the required context from the context dropdown menu and then click **Configuration**. The Context Configuration window enables you to configure context-based security policies. From the Context Configuration window, you can configure context-related interfaces, security policies, NAT, IPS, routing, building blocks, device administration, properties, and the startup wizard.

Context Monitoring

You can monitor specific context-related statistics by selecting a context from the Context dropdown menu and then clicking **Monitoring**. From the Context Monitoring window, you can monitor context interfaces, routing, administration, connections, logging, and IP audit statistics.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

- **ASDM is a browser-based tool used to configure your security appliance.**
- **Minimal setup on the security appliance is required to run ASDM.**
- **ASDM contains several tools in addition to the GUI to help you configure your security appliance.**
- **ASDM wizards can be used to create site-to-site and remote access VPNs.**
- **ASDM wizards make configuring the security appliance easier.**

SNPA v4.0—17-40

Lesson 18

AIP-SSM—Getting Started

Overview

This lesson describes the Advanced Inspection and Prevention Security Services Module (AIP-SSM). The lesson describes how to load Intrusion Prevention System (IPS) software on the AIP-SSM module, initialize the module with the **setup** command, and define an IPS modular policy on a security appliance via Cisco Adaptive Security Device Manager (ASDM).

Objectives

Upon completing this lesson, you will be able to initialize an AIP-SSM module. This ability includes being able to meet these objectives:

- Describe the AIP-SSM module

- Compare and contrast promiscuous and in-line modes

- Explain the steps necessary to load software on a AIP-SSM

- Configure the AIP-SSM setup parameters

- Configure an IPS modular policy on a security appliance via ASDM

AIP-SSM Overview

This topic provides on overview of the AIP-SSM module.
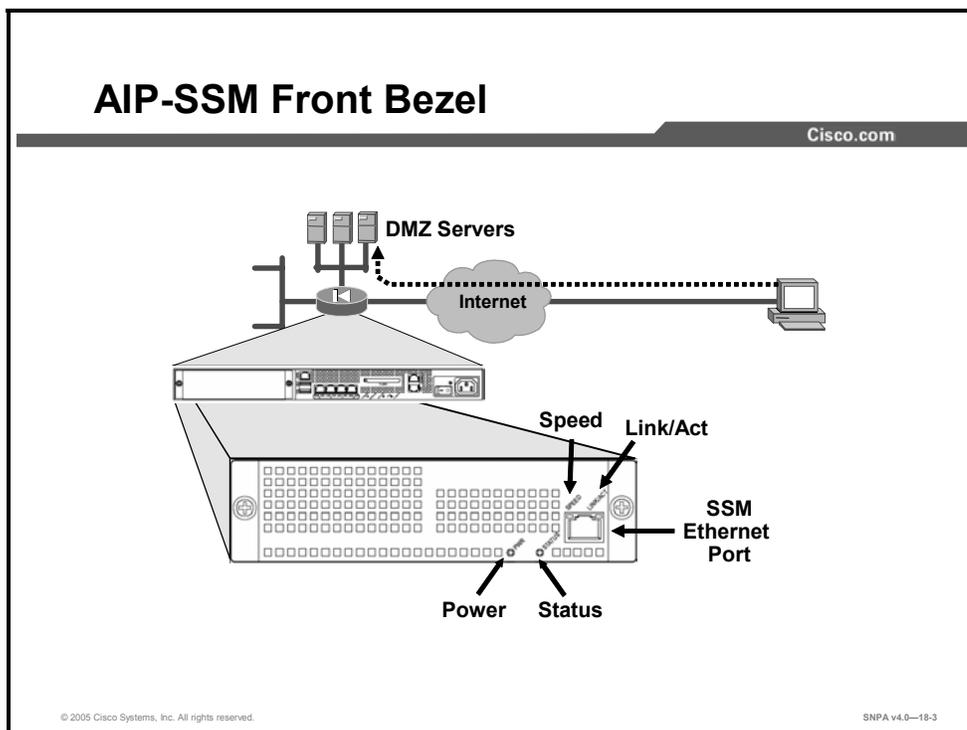
AIP-SSM Front Bezel

There are two AIP-SSM models, the AIP-SSM-10 and the AIP-SSM-20. Both modules appear identical, but the AIP-SSM-20 has a faster processor and more memory than the AIP-SSM-10. Only one module can populate the slot at a time. On the front bezel of the AIP-SSM module, there are four LEDs and one 10/100/1000 Ethernet port. The table lists the states of the AIP-SSM LEDs.

States of AIP-SSM LEDs

LED	Color	State	Description
Power	Green	On	On when the security appliance has power.
Status	Green	Flashing	Flashing when the power-up diagnostics are running or the system is booting.
		Solid	Green when the system has passed power-up diagnostics.
	Amber	Solid	Amber when the power-up diagnostics have failed.
Speed	Green	Flashing	Flashing when there is network activity.
Link/Act	Green	Solid	Green when data is passing through the interface.

Remove power to the ASA 5500 before installing or removing the AIP-SSM module.

AIP-SSM Ethernet Connections

DMZ Servers

Internet

AIP-SSM

ASA 5500

AIP-SSM

IPS
Data channel
Control
channel

SW Download
and ASDM
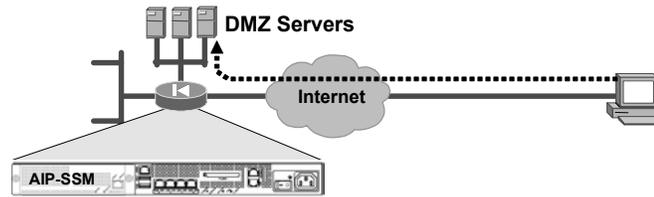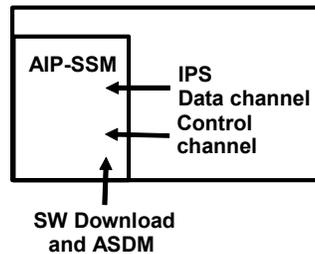
SNPA v4.0—18-4

The AIP-SSM supports an internal Gigabit Ethernet and a 10/100 Ethernet interface to the ASA 5500 Family main card. The Gigabit Ethernet interface is the primary IPS data-path interface for both inline and promiscuous IPS packets. An internal 10/100 Ethernet interface provides a control channel to the ASA 5500 main card. The external 10/100/1000 Ethernet interface is primarily used for downloading AIP-SSM software and for ASDM access to the AIP-SSM module.

AIP-SSM: Modes of Operation

Cisco.com

DMZ Servers

Internet

AIP-SSM

DMZ

Promiscuous
copy
of traffic

IDS

Intrusion Detection

DMZ

Inline
actual traffic

IPS

Intrusion Prevention
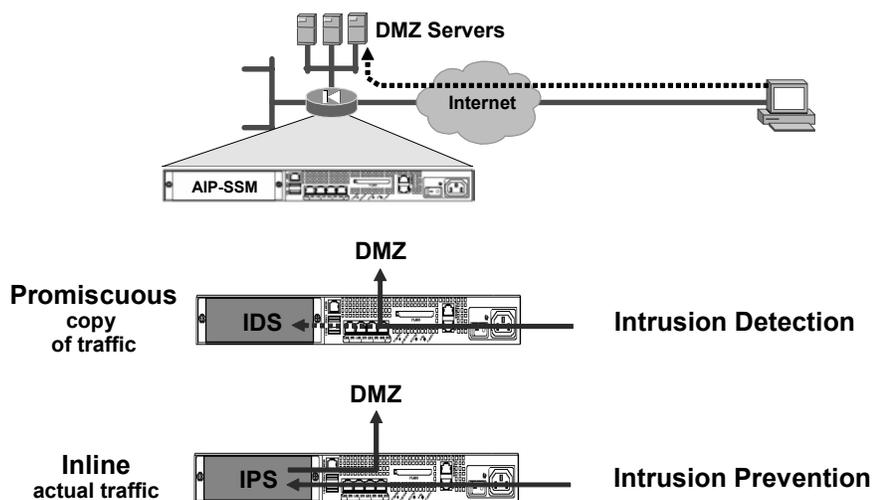
SNPA v4.0—18-5

An AIP-SSM can be configured to operate in one of two IPS modes, promiscuous or inline. In promiscuous mode, the IPS module is not in the traffic packet flow. You can configure a security policy (using standard rules and access control lists [ACLs]) to identify traffic that will be copied and passed to the AIP-SSM module. The AIP-SSM module performs analysis of the traffic. A significant benefit of operating an IPS module in promiscuous mode is that the IPS module does not affect the packet flow. There are no performance or operational reliability issues with the forwarded traffic. The drawback to operating in a promiscuous mode, however, is that the AIP-SSM module may not stop malicious traffic from reaching its intended target. The response actions implemented by modules in promiscuous mode are typically post-event responses and often require assistance from other networking devices, such as routers and firewalls, to respond to an attack. The argument can be successfully made that modules operating in promiscuous mode cannot prevent an attack, but can only react. Most IPS products on the market today operate in promiscuous mode.

Operating in an inline mode, the IPS module is inserted directly into the traffic flow. You configure a security policy, using standard rules and ACLs, to identify traffic that will be passed directly to the AIP-SSM module. An inline IPS module sits in the data path, allowing the sensor to stop attacks by dropping malicious traffic before it reaches the intended target.

The AIP-SSM module not only processes information on the packet "envelope" (Layers 3 and 4), but also analyzes the contents, or payload, of the packets for more sophisticated embedded attacks (Layers 3 to 7). This deeper analysis allows the system to identify and block attacks that would normally pass through a traditional firewall device.

AIP-SSM: Failure Modes

DMZ Servers

Internet

AIP-SSM

DMZ

IPS — Fail-Open

DMZ
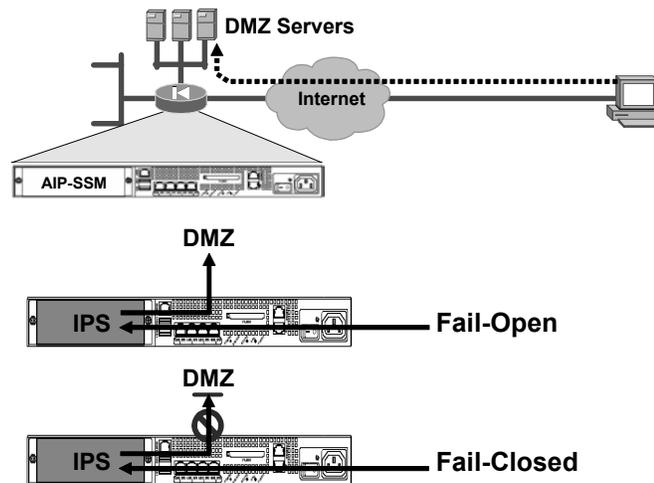
IPS — Fail-Closed

SNPA v4.0—18-6

You also need to configure what action to take if the AIP-SSM module fails. **"**Fail-open" or "fail-closed" refers to what should happen to the traffic flow if the AIP-SSM fails for any reason, either a hardware or a software malfunction. With fail-open configured, if the AIP-SSM module fails, traffic will continue to flow. When operating in promiscuous mode, AIP-SSM modules are typically configured for fail-open. With fail-closed enabled, traffic will cease flowing if the IPS software fails for any reason.

Initializing the AIP-SSM Module

Cisco.com
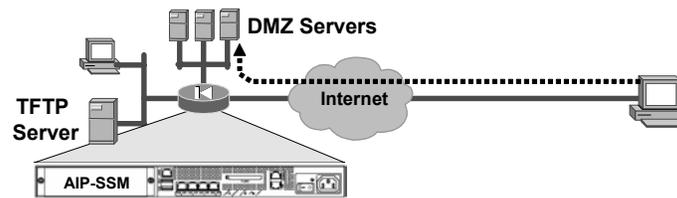
Bootstrapping the AIP-SSM:

- **Load the IPS software (if necessary)**
- **Configure initial setup of AIP-SSM module**
- **Configure a security policy on ASA security appliance**

SNPA v4.0—18-7

Before the AIP-SSM module can start to inspect and analyze traffic, three steps need to be performed. You should verify, or load and verify, the IPS operating software on the AIP-SSM module. After verifying the IPS software, you should configure the initial setup of the AIP-SSM module. Lastly, you should configure an IPS policy for the ASA 5500. Each of these steps is discussed in more depth later in this lesson.

AIP-SSM SW Loading

This topic describes loading and verifying AIP-SSM Software.

AIP-SSM Module: No Software

Cisco.com
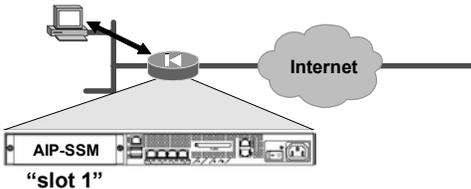
```
asa1# show module 1 detail
Getting details from the Service Module, please wait...
Unable to read details from slot 1
ASA 5500 Series Security Services Module-10
Model:               ASA-SSM-10
Hardware version:    1.0
Serial Number:       12345678
Firmware version:    1.0(7)2
Software version:
Status:              Init
```

SNPA v4.0—18-9

You can use the **show module 1 detail** command to view module 1 configuration. You can view such statistics as hardware version, software version, firmware version, and status of the AIP-SSM module. The table lists the parameters of the command.

```
show module [all | slot [details | recover]]
```

all	Shows information for SSM, slot 1.
details	Shows additional version information.
recover	Shows the settings for the **hw-module module recover** command.
slot	Specifies the SSM slot information.

The output fields of the **show module** command are as follows:

- **Model:** The model of this SSM
- **Serial Number:** The serial number of the SSM
- **Hardware version:** The hardware version of the SSM
- **Firmware version:** The firmware version of the SSM
- **Software version:** The software version of the SSM

- **Status:** The status of the module, as follows:

  — **Initializing:** The SSM is being detected and the control communication is being initialized by the system.

  — **Up:** The SSM has completed initialization by the system.

  — **Unresponsive:** The system encountered an error communicating with this SSM.

  — **Reloading:** The SSM is reloading.

  — **Shutting:** The SSM is shutting down.

  — **Shut Down:** The SSM is shut down.

  — **Recover:** The SSM is attempting to download a recovery image.

In the example in the figure, the AIP-SSM present is an SSM-10 model. Notice there is no software present on the module and the module is in the status of trying to initialize.

TFTP Download Information

AIP-SSM

Internet

TFTP Server

.1

.10
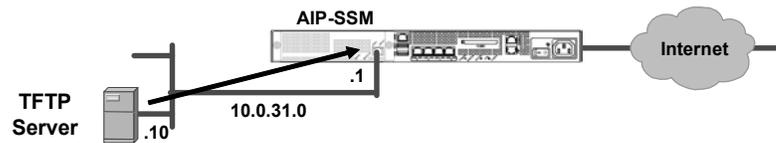
10.0.31.0

TFTP server IP address and image path

- **SSM Ethernet port IP address**
- **SSM Ethernet port 802.1q VLAN ID**
- **SSM Ethernet port default gateway address**

```
asa1(config)# hw module 1 recover configure
Image URL [tftp://0.0.0.0/]: tftp://10.0.31.10/AIP-SSM-K9-sys-1.1-a-5.0-0.22.img
Port IP Address [0.0.0.0]: 10.0.31.1
VLAN ID [0]:
Gateway IP Address [0.0.0.0]:
```

SNPA v4.0—18-10

You can use the **hw module 1 recover** command to load a recovery software image to the AIP-SSM from a Trivial File Transfer Protocol (TFTP) server. This is a two-step process. You must first define the SSM interface and TFTP server network parameters, and then initiate the download.

Adding the **configure** keyword to the command enables you to define the SSM and TFTP server network parameters. In the example in the figure, the TFTP server IP address is 10.0.31.10, and the external AIP-SSM Ethernet connector IP address is 10.0.31.1. The TFTP server will download the AIP-SSM-K9-sys-1.1-a-5.0-0.22.img image file to the AIP-SSM module.

The table shows the parameters of the **hw module 1 recover** command.

```
hw module module slot recover {boot | stop | configure [url tfp_url |
ip port_ip_address | gateway gateway_ip_address | vlan vlan_id]}
```

boot	Initiates recovery of this SSM and downloads a recovery image according to the configuration settings. The SSM then reboots from the new image.
configure	Configures the network parameters to download a recovery image. If you do not enter any network parameters after the **configure** keyword, you are prompted for the information.
gateway *gateway_ip_address*	Sets the gateway IP address for access to the TFTP server through the SSM management interface.
ip port_*ip_address*	Sets the IP address of the SSM management interface.
slot	Specifies the SSM slot number.
stop	Stops the recovery action, and stops downloading the recovery image. The SSM boots from the original image.
url *tfp_url*	Sets the URL for the image on a TFTP server, in the following format: **tftp://**server/[path**/**]filename.
vlan *vlan_id*	Sets the VLAN ID for the management interface.

Recover IPS Image

```
asa1(config)# debug module
debug module-boot  enabled at level 1
asa1(config)# hw module 1 recover boot

The module in slot 1 will be recovered.  This may
erase all configuration and all data on that device and
attempt to download a new image for it.
Recover module in slot 1? [confirm]
Recover issued for module in slot 1
asa1(config)# %The module in slot 1 is unresponsive.
%The module in slot 1 is recovering.
Slot-1 8> tftp AIP-SSM-K9-sys-1.1-a-5.0-0.22.img@10.0.31.10
Slot-1 9> !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!
%The module in slot 1 is recovering.
Slot-1 10>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!
........
Slot-1 79> !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 80> Received 23140374 bytes
Slot-1 81> Launching TFTP Image...
%The module in slot 1 is recovering.
%The module in slot 1 is recovering.
%The module in slot 1 is recovering.
%The module in slot 1 is recovering.
Slot-1 82> Launching BootLoader...
%The module in slot 1 is recovering.
%The module in slot 1 is recovering.
```

SNPA v4.0—18-11

You can use the **hw module 1 recover boot** command to initiate the TFTP download of the image defined in the **hw module 1 recover configure** command. To aid in the download, you can enable the **debug module** command. A sample of a download is displayed in the example in the figure. The full debug output was truncated to fit into the window. Downloading and launching the image, launching the bootloader, and recovering the module takes approximately five minutes to complete.

AIP-SSM Initialized
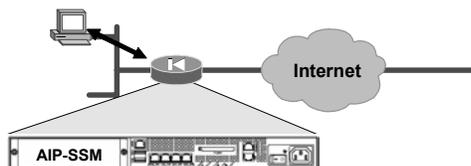
```
asa1# show module 1

Mod Card Type                                        Model           Serial No.
--- ---------------------------------------------- --------------- ----------
  1 ASA 5500 Series Security Services Module-10 ASA-SSM-10      12345678

Mod MAC Address Range             Hw Version  Fw Version   Sw Version
--- ----------------------------- ---------- ------------ ------------
  1 000b.fcf8.0170 to 000b.fcf8.0170 1.0         1.0(7)2      5.0(0.22)S129.0

Mod Status
--- ------------------
  1 Up
```

SNPA v4.0—18-12

Once the SSM module is initialized, you can use the **show module 1** command to view the status of the module. From the show module 1 window, you can view the model type, Media Access Control (MAC) address, serial number, hardware version, firmware version, and software version of the AIP-SSM module. You can also determine the status of the module. In the example in the figure, notice that the module is in the Up status and IPS software version 5.0(0.22)S129.0 is loaded on the module.

Initiate a Session with the AIP-SSM
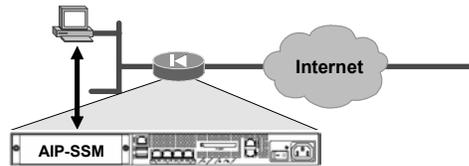
```
asa1# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.

login: cisco
Password: <cisco>
You are required to change your password immediately (password aged)
Changing password for cisco
(current) UNIX password: <cisco>
New password: <training>
Retype new password: <training>
………….
sensor#
```

SNPA v4.0—18-13

If the SSM is in the Up status, you can open a Telnet session with the module via the security appliance command line. To initiate a Telnet session, enter the **session 1** command at the command-line interface (CLI) command prompt. Entering the **session 1** command for the first time, you are prompted for the default login prompt, username **cisco** and password **cisco**. After entering the default login and password, you are immediately prompted to change the password. In the example in the figure, the password was changed to **training**. After changing the password, the default **sensor#** command prompt is displayed**.** To end a session, enter **exit** or **Ctrl+Shift+6** followed by the **x** key.

Session Setup Default

```
sensor# setup

    --- System Configuration Dialog ---

Current Configuration:

service host
network-settings
host-ip 10.1.9.201/24,10.1.9.1
host-name sensor
telnet-option disabled
ftp-timeout 300
login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 443
exit
```

SNPA v4.0—18-14

After installing and loading software on the AIP-SSM module, you must initialize the AIP-SSM module using the **setup** command. With the **setup** command, you can configure basic AIP-SSM settings, including the host name, IP interfaces, Telnet server, web server port, access control lists, and time settings. The example in the figure displays the default setup parameters. Notice that the default IP address of the external Ethernet connector is 10.1.9.201/24.

Session Setup Command

Cisco.com

```
sensor# setup
………….
Continue with configuration dialog?[yes]: <yes>
Enter host name[sensor]: sensor1
Enter IP interface[10.1.9.201/24,10.1.9.1]: 10.0.1.41/24,10.0.1.1
Enter telnet-server status[disabled]:
Enter web-server port[443]:
Modify current access list?[no]: yes
Current access list entries:
  No entries
Permit: 10.0.1.0/24
Permit:
………….

[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.

Enter your selection[2]: 2
Warning: Reboot is required before the configuration change will take effect
Configuration Saved.
Warning: The node must be rebooted for the changes to go into effect.
Continue with reboot? [yes]: yes
```

To communicate with ASDM, you may need to change some of the default setup parameters such as the IP interface and current access list. A description of the **setup** command parameters is as follows:

- **Enter host name[sensor]:** Name of the sensor. The host name can be a string of 1 to 64 characters that matches the pattern ^[A-Za-z0-9_/-]+$. The default is sensor. You receive an error message if the name contains a space or exceeds 64 alphanumeric characters.

- **Enter IP interface [10.1.9.201/24, 10.1.9.1]:** IP address of the external AIP-SSM Ethernet interface. The default is 10.1.9.201. The default mask corresponding to the IP address is /24, or 255.255.255.0. The default gateway address is 10.1.9.1.

- **Enter telnet-server status[disabled]:** Enables or disables Telnet for remote access to the sensor. Telnet is not a secure access service and therefore is disabled by default.

- **Enter web-server port[443]:** TCP port used by the web server. The default is 443 for Hypertext Transfer Protocol secure (HTTPS). You receive an error message if you enter a value out of the range of 1 to 65535.

- **Modify current access list?[no]:** IP address of the hosts or networks that have permission to access the sensor. By default there are no entries.

In the example in the figure, the IP address of the external Ethernet connector was changed to 10.0.1.41/24. Hosts on the 10.0.1.0/24 subnet are permitted to access the module.

Show Module Detail Command

```
asa1# show module 1 detail
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-10
Model:            ASA-SSM-10
Hardware version: 1.0
Serial Number:    0
Firmware version: 1.0(7)2
Software version: 5.0(0.22)S129.0
Status:           Up
Mgmt IP addr:     10.0.1.41

Mgmt web ports:   443

Mgmt TLS enabled: true
```

SNPA v4.0—18-16

You can use the **show module 1 detail** command to view AIP-SSM hardware and software details, including the remote management configuration. In the example in the figure, a device manager can access the AIP-SSM module through the AIP-SSM external interface at IP address is 10.0.1.41, the AIP-SSM web server port is 443, and management Transport Layer Security (TLS)/Secure Socket Layer (SSL) is enabled.

Initial IPS ASDM Configuration

This topic describes how to access the AIP-SSM with ASDM.
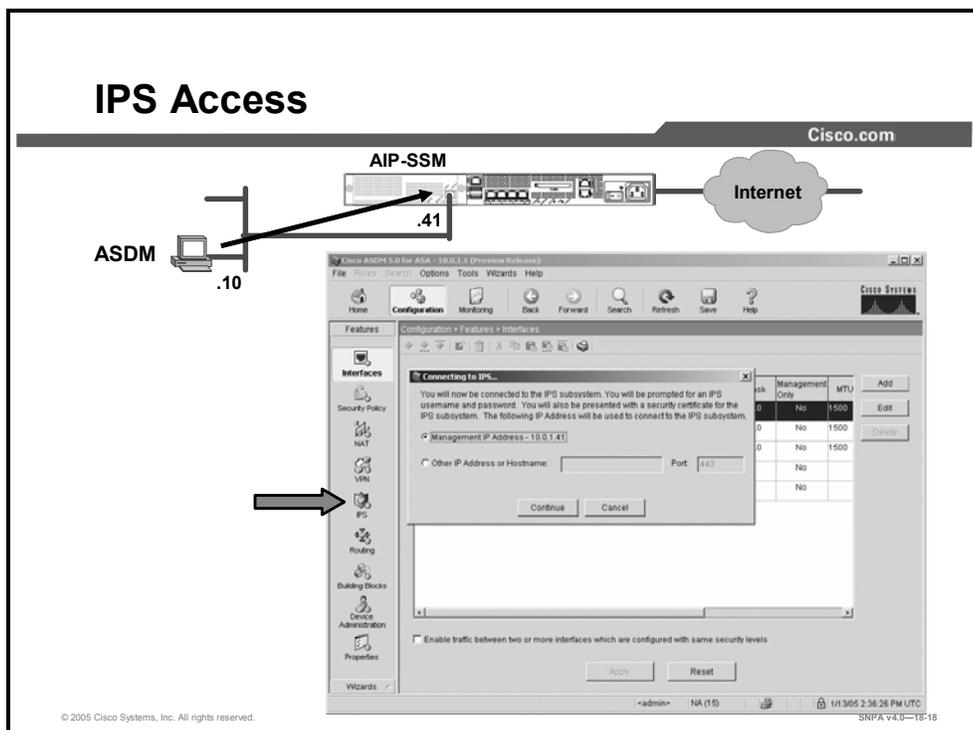
After installing the AIP-SSM module, you initialized the module using the **setup** command from the CLI. With the **setup** command, you configured basic sensor settings, including the host name, IP interfaces, web server port, access control lists, and time settings. After initializing the AIP-SSM module, you can now communicate with the module, using ASDM. The IPS icon will not be present on ASDM until the IPS software is installed and configured on the AIP-SSM module.

To access the AIP-SSM module from ASDM, click the **IPS** icon under the features column. The Connecting to IPS popup window appears. The IP address referenced by the Management IP Address prompt in the popup window refers to the IP address of the external Ethernet interface of the AIP-SSM module. An option is provided in this dialog to enter a different IP address, in case you are accessing the IPS sensor from behind a Network Address Translation (NAT) device. ASDM can only manage the AIP-SSM card in the same chassis as the ASA that ASDM is started from. Click the **Management IP Address** button and then click **Continue**. If a route exists between the ASDM PC and the external Ethernet interface on the AIP-SSM module, the AIP-SSM session login prompt should open.

You can configure intrusion prevention either using the ASDM or through the CLI.

IPS Login
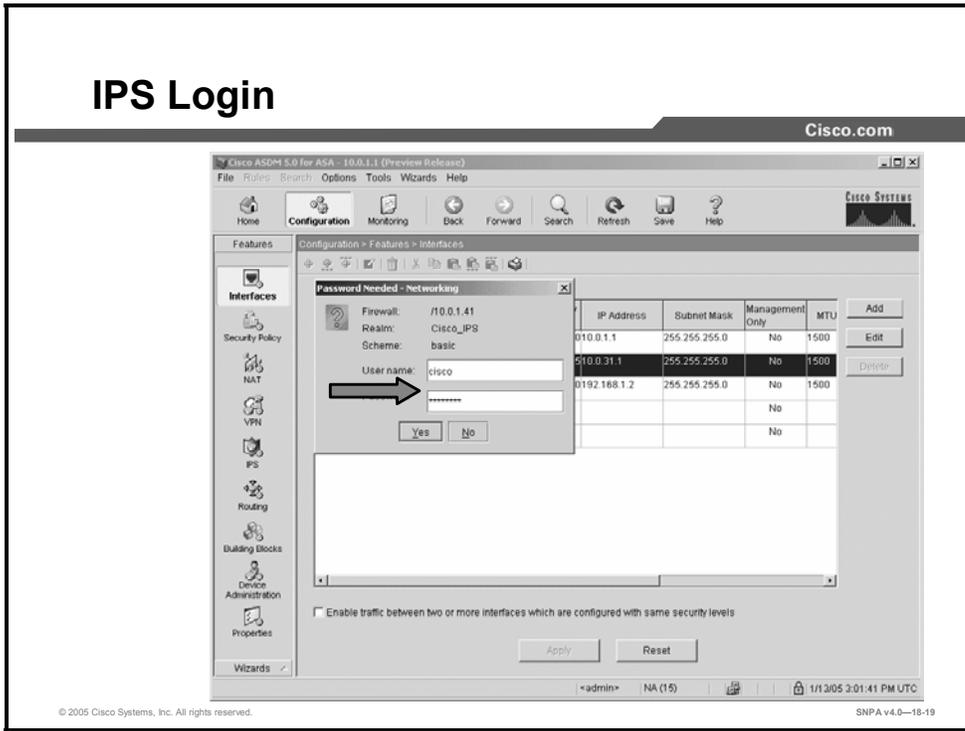
If connectivity exists between the PC and the AIP-SSM, you are prompted for your IPS username and password. Separate authentication is required by the IPS software. This allows for separation of security appliance management and IPS management. Type your IPS username and password. Click **Yes** to continue.

IPS Configuration Menu

SNPA v4.0—18-20
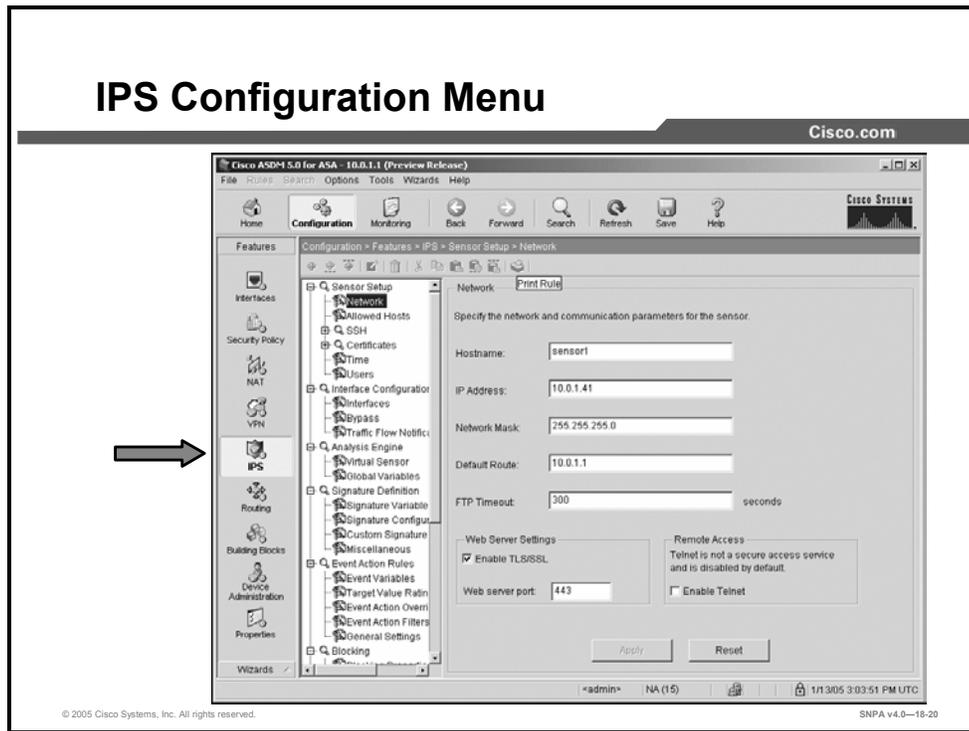
Use the Network window to specify network and communication parameters for the AIP-SSM module. After you use the **setup** command to initialize the sensor, the network and communication parameter values appear in the Network window. If you need to change these parameters, you can do so from the Network window.

Allowed Administrative Hosts

SNPA v4.0—18-21
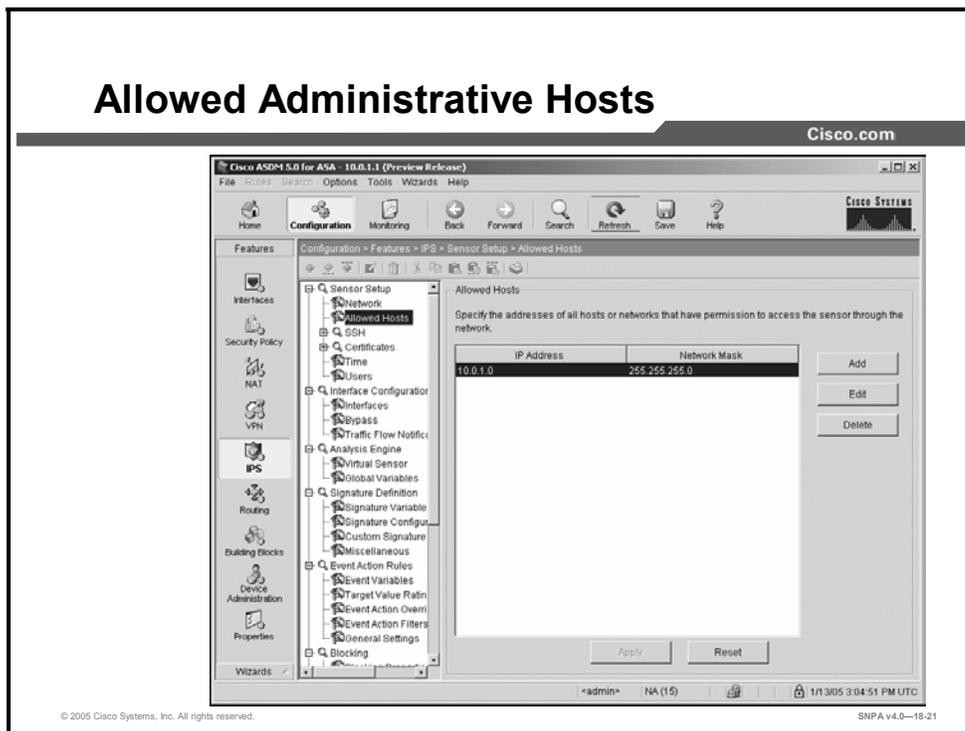
Use the Allowed Hosts window to specify hosts or networks that have permission to access the AIP-SSM module. After you use the **setup** command to initialize the AIP-SSM module, the allowed hosts parameter values appear on the Allowed Hosts window. If you need to change these parameters, you can do so from the Allowed Hosts window. You must add the management host, such as ASDM, Intrusion Detection System Device Manager (IDM), IPS Management Center (MC) and the monitoring host, such as IPS Security Monitor, to the allowed hosts list; otherwise, you will not be able to communicate with the AIP-SSM module.

Add Users

SNPA v4.0—18-22
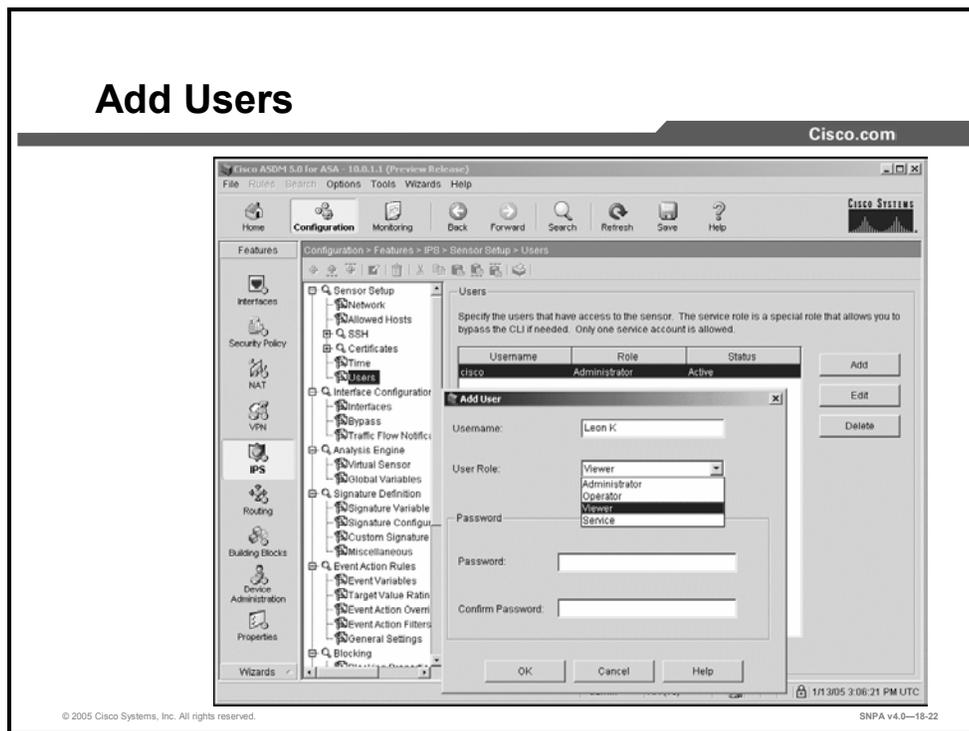
ASDM permits only one user to log in at a time. If another user tries to log in, a message says the first user is logged in. You can create and remove users from the AIP-SSM. Each user is associated with a role that controls what that user can and cannot modify.

There are four user roles:

- **Viewers:** Can view configuration and events, but cannot modify any configuration data except their user passwords.

- **Operators:** Can view everything and can modify the following options:

    — Signature tuning (priority, disable, or enable)

    — Virtual sensor definition

    — Managed routers

    — Their user passwords

- **Administrators:** Can view everything and can modify all options that operators can modify, in addition to the following:

    — Sensor addressing configuration

    — List of hosts allowed to connect as configuration or viewing agents

    — Assignment of physical sensing interfaces

    — Enable or disable control of physical interfaces

    — Add and delete users and passwords

    — Generate new SSH host keys and server certificates

- **Service:** Only one user with service privileges can exist on an AIP-SSM module. The service role is a special role that allows a service user to bypass the CLI if needed. Only one service account is allowed.

Configure a Security Policy on the ASA Security Appliance

This topic describes how to configure an IPS service policy on the ASA security appliance.
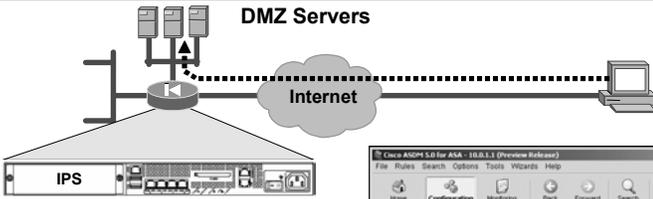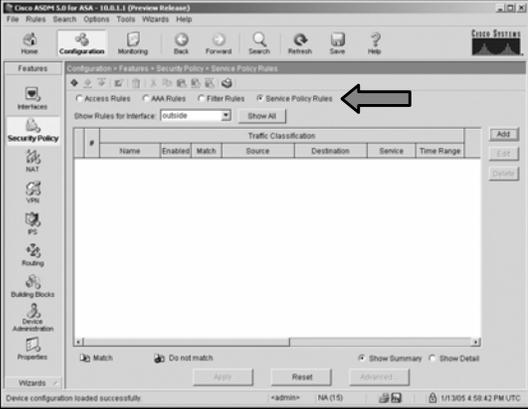
The last step in the process is to create a security policy on the ASA security appliance. A security policy enables the ASA security appliance to prefilter, then pass selected traffic to the AIP-SSM module for inspection and analysis. This level of interaction between the ASA security appliance and AIP-SSM module enables the IPS system to operate at greater efficiency. The AIP-SSM module analyzes only a subset of the total bandwidth, the relevant traffic, and filters out nonrelevant traffic. You can apply a security policy to an interface or globally to every interface.

To create an IPS service policy from ASDM, select the **Security Policy** Icon and click the **Service Policy Rules** button.

Create a Service Policy
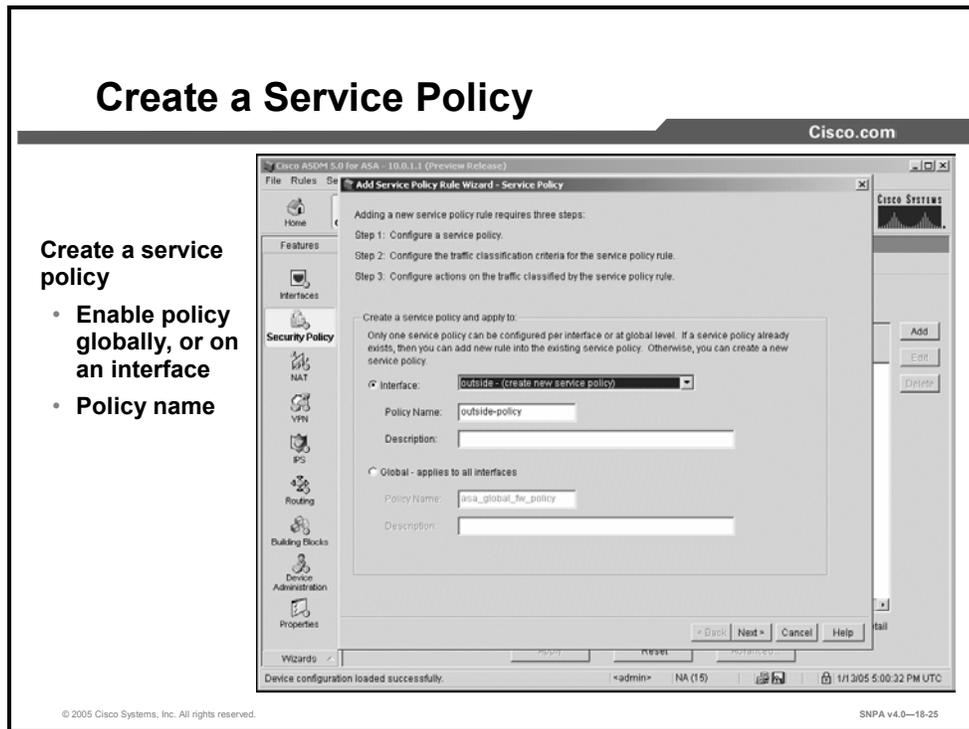
The Add Service Policy Rule Wizard dialog box guides you through the addition of a new service policy rule. The new security policy rule can be applied to a specific interface, such as the outside or inside interface, or can be applied globally to all interfaces.

A description of the fields in the **Create a service policy and apply to:** group box is as follows:

- **Interface radio button:** Applies the rule to a specific interface. This selection is required if you want to match traffic based on the source or destination IP address using an ACL.

- **Interface drop-down list:** Specifies the interface to which the rule applies.

- **Description field:** Provides a text description of the policy.

- **Global - applies to all interfaces radio button:** Applies the rule to all interfaces.

- **Policy Name box:** Specifies the name of the global service policy. Only one global service policy is allowed and it cannot be renamed.

- **Description box:** Provides a text description of the policy.

Identify a Class of Traffic

Class of traffic
- **Create a traffic class**
- **Defining traffic matching criteria**

SNPA v4.0—18-26

After you define a service policy, you define a traffic class. You define the criteria used by the ASA security appliance to identify which traffic will be routed to the AIP-SSM module for inspection and analysis. The Traffic Classification Criteria dialog box enables you to specify the criteria you want to use to match traffic to which the security policy rule applies. A description of the fields is as follows:

- **Create a new traffic class:** Identifies the name of the new traffic class

- **Description:** Provides a text description of the new traffic class

- **Traffic match criteria:** The available matching criteria choices are as follows:

    — **Default Inspection Traffic:** Uses the criteria specified in the default inspection traffic policy.

    — **Source and Destination IP Address (uses ACL):** Matches traffic based on the source and destination IP addresses, using an ACL. This selection is only available if you apply the rule to a specific interface using an interface service policy.

    — **Tunnel Group:** Matches traffic based on the tunnel group. If a tunnel group is selected as one match criteria, a second criteria can also be selected.

    — **TCP or UDP Destination Port:** Matches traffic based on the TCP or UDP destination port.

    — **RTP Range:** Matches traffic based on a range of Real-Time Transport Protocol (RTP) ports.

    — **IP DiffServ CodePoints (DSCP):** Matches traffic based on the Differentiated Services model of quality of service (QoS).

    — **IP Precedence:** Matches traffic based on the IP precedence model of QoS.

    — **Any traffic:** Matches all traffic regardless of the traffic type.

In the example in the figure, the administrator selected the **Source and Destination IP Address (uses ACL)** button. The traffic inspected and analyzed by the AIP-SSM module is identified by the source and destination addresses.

Define Traffic Matching Criteria

The Source and Destination Address dialog box appears when you select **Source and Destination IP Address (uses ACL)** on the Traffic match criteria dialog box. This dialog window enables you to identify the traffic to which a service policy rule applies based on the IP address of the sending or receiving host. In the example in the figure, the traffic criteria is a packet with any source IP address from the outside destined to the DMZ subnet 172.16.1.0/24.

Define IPS Policy

Cisco.com

DMZ Servers
172.16.1.0/24

Internet

IPS

Create IPS Policy:
- **Mode**
  - **Inline**
  - **Promiscous**
- **IPS card failure**
  - **Permit traffic**
  - **Close traffic**

SNPA v4.0—18-28

The Intrusion Prevention tab enables you to configure the IPS action to take on the selected traffic class. This window appears only if IPS software and AIP-SSM hardware is installed in the security appliance. The fields in the Intrusion Prevention area are as follows:

- **Enable IPS for this traffic flow:** This check box enables or disables intrusion prevention for the traffic flow. When this check box is selected, the other parameters in this window become active.

- **Mode:** This group box configures the operating mode for intrusion prevention.

  — **Inline Mode:** This radio button selects Inline Mode, in which a packet is directed to IPS. The packet might be dropped as a result of the IPS operation.

  — **Promiscuous Mode:** This radio button selects Promiscuous Mode, in which IPS operates on a duplicate of the original packet. The original packet cannot be dropped.

- **If IPS card fails, then:** Configures the action to take if the IPS card becomes inoperable.

  — **Permit traffic:** The radio button permits traffic if the IPS card fails.

  — **Close traffic:** The radio button blocks traffic if the IPS card fails.

Apply or View Service Policy Rule

DMZ Servers
172.16.1.0/24 ← Any Host

Internet

IPS

Configuration > Features > Security Policy > Service Policy Rules

Access Rules   AAA Rules   Filter Rules   Service Policy Rules

Show Rules for Interface: outside   Show All

#	Traffic Classification							
	Name	Enabled	Match	Source	Destination	Service	Time Range	
Interface: outside, Policy: outside-policy								
1	outside-class	☑		any	172.16.1.0/24	tcp	-- Not Applie...	

Add
Edit
Delete

Match   Do not match   Show Summary   Show Detail

Apply   Reset   Advanced...

SNPA v4.0—18-29

The last step is to apply the service policy rule. Click **Apply** to initiate the new IPS service policy. In the example in the figure, the outside traffic class, defined as those packets from any source to a destination address of 172.16.1.0/24 will be inspected and analyzed by the AIP-SSM module.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

- **There are two AIP-SSM models, SSM-10 and SSM-20.**
- **If there is no IPS software on the AIP-SSM, or if it is corrupted, use the** hw module 1 recover **command to load the initial IPS software image.**
- **Use the** session **command to configure the initial AIP-SSM setup .**
- **Use ASDM, or CLI, to configure a modular policy for IPS inspection.**

SNPA v4.0—18-31

Lesson 19

Managing Security Appliances

Overview

This lesson describes how to secure system access to the security appliance and how to configure and use local user authentication and command authorization. Password recovery is covered as well as file management. The lesson also describes how to upgrade the security appliance image and activation keys.

Objectives

Upon completing this lesson, you will be able to secure and upgrade system access to the security appliance and recover from possible problems. This ability includes being able to meet these objectives:

■ Configure Telnet access to the security appliance console

■ Configure SSH access to the security appliance console

■ Configure command authorization

■ Recover security appliance passwords using general password recovery procedures

■ Use TFTP to install and upgrade the software image on the security appliance

Managing System Access

This topic describes how to configure a secure remote connection to a security appliance console.

Configuring Telnet Access to the Security Appliance Console
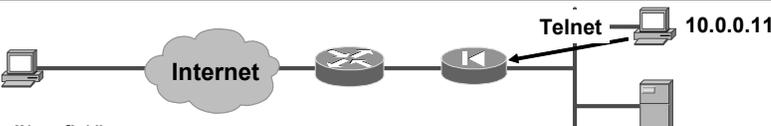
```
firewall(config)#
telnet {{hostname | IP_address mask interface_name} |
{IPv6_address interface_name} | {timeout number}}

firewall(config)#
telnet timeout minutes
```
• Sets the maximum time a console Telnet session can be idle before being logged off by the security appliance.

```
firewall(config)#
{passwd | password} password [encrypted]
```
• Sets the password for Telnet access to the security appliance.

```
fw1(config)# telnet 10.0.0.11 255.255.255.255 inside
fw1(config)# telnet timeout 15
fw1(config)# passwd telnetpass
```

SNPA v4.0—19-3

The serial console permits a single user to configure the security appliance, but often this is not convenient for a site with more than one administrator. By configuring console access via Telnet, you can allow a maximum of five concurrent Telnet connections per context, if available, with a maximum of 100 connections divided between all contexts.

You can enable Telnet to the security appliance on all interfaces. However, the security appliance requires that all Telnet traffic to the outside interface be IPSec protected. To enable a Telnet session to the outside interface, configure IPSec on the outside interface to include IP traffic generated by the security appliance, and enable Telnet on the outside interface.

The following are the Telnet configuration commands:

■ **telnet**: Specifies which hosts can access the security appliance console via Telnet. Up to 16 hosts or networks can be specified.

■ **telnet timeout**: Sets the maximum time a console Telnet session can be idle before being logged off by the security appliance. The default is five minutes.

■ **password**: Sets the password for Telnet access to the security appliance. The default value is cisco.

In the figure, host 10.0.0.11 on the internal interface is allowed to access the security appliance console via Telnet using the password telnetpass. If the Telnet session is idle more than fifteen minutes, the security appliance closes it.

The syntaxes for the Telnet configuration commands are as follows:

```
telnet {{hostname | IP_address mask interface_name} |
{IPv6_address interface_name} | {timeout number}} {passwd |
password} password [encrypted]
```

hostname	Specifies the name of a host that can access the Telnet console of the security appliance.
interface_name	Specifies the name of the network interface to Telnet to.
IP_address	Specifies the IP address of a host or network authorized to log in to the security appliance.
IPv6_address	Specifies the IPv6 address or prefix authorized to log in to the security appliance.
mask	Specifies the netmask associated with the IP address.
timeout *number*	Specifies the number of minutes that a Telnet session can be idle before being closed by the security appliance; valid values are from 1 to 60 minutes.
encrypted	(Optional) Specifies that the password is in encrypted form. The password is saved in the configuration in encrypted form, so you cannot view the original password after you enter it. If for some reason you need to copy the password to another security appliance but do not know the original password, you can enter the **passwd** command with the encrypted password and this keyword. Normally, you only see this keyword when you enter the **show running-config passwd** command.
password	Sets the password as a case-sensitive string of up to 16 alphanumeric and special characters. You can use any character in the password except a question mark or a space.

Viewing and Disabling Telnet

firewall#

```
show running-config telnet [timeout]
```

- Displays IP addresses permitted to access the security appliance via Telnet.

firewall(config)#

```
clear configure telnet
```

- Removes the Telnet connection and the idle timeout from the configuration.

firewall#

```
who [local_ip]
```

- Enables you to view which IP addresses are currently accessing the security appliance console via Telnet.

firewall#

```
kill telnet_id
```

- Terminates a Telnet session.

SNPA v4.0—19-4

The following commands enable you to view and clear Telnet configuration and Telnet sessions:

- **show running-config telnet**: Displays the current list of IP addresses authorized to access the security appliance via Telnet. You can also use this command to display the number of minutes that a Telnet session can remain idle before being closed by the security appliance.

- **clear configure telnet**: Removes the Telnet connection and the idle timeout from the configuration.

- **who**: Enables you to view which IP addresses are currently accessing the security appliance console via Telnet.

- **kill**: Terminates a Telnet session. When you kill a Telnet session, the security appliance lets any active commands terminate and then drops the connection without warning the user.

SSH Connections to the Security Appliance

SSH connections to the security appliance:

- **Provide secure remote access**
- **Provide strong authentication and encryption**
- **Require RSA key pairs for the security appliance**
- **Require AES or 3DES activation keys**
- **Allow up to five SSH clients to simultaneously access the security appliance console**
- **Use the Telnet password for local authentication**

SNPA v4.0—19-5

Secure Shell (SSH) provides another option for remote management of the security appliance. SSH provides a higher degree of security than Telnet, which provides lower-layer encryption and application security. The security appliance supports the SSH remote functionality, which provides strong authentication and encryption capabilities. SSH, an application running on top of a reliable transport layer such as TCP, supports logging onto another computer over a network, executing commands remotely, and moving files from one host to another.

Both ends of an SSH connection are authenticated, and passwords are protected by being encrypted. Since SSH uses Rivest, Shamir, and Adleman (RSA) public key cryptography, an Internet encryption and authentication system, you must generate an RSA key pair for the security appliance before clients can connect to the security appliance console. Your security appliance must also have an Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES) activation key.

The security appliance allows up to five SSH clients to simultaneously access its console. You can define specific hosts or networks that are authorized to initiate an SSH connection to the security appliance, as well as how long a session can remain idle before being disconnected.

Note	The security appliance SSH implementation provides a secure remote shell session without IPSec, and only functions as a server, which means that the security appliance cannot initiate SSH connections.

Configuring SSH Access to the Security Appliance Console

firewall(config)#

```
crypto key zeroize {rsa | dsa}
[label key-pair-label] [default]
[noconfirm]
```

• **Removes any previously generated RSA keys**

firewall(config)#

```
crypto key generate rsa [usage-keys
| general-keys] [label key-pair-
label] [modulus size] [noconfirm]
```

• **Generates an RSA key pair**

firewall(config)#

```
write memory
```

• **Saves the CA state**

firewall(config)#

```
ssh {ip_address mask |
ipv6_address/prefix} interface
```

• **Specifies the host or network authorized to initiate an SSH connection**

firewall(config)#

```
domain-name name
```

• **Configures the domain name**

firewall(config)#

```
ssh timeout number
```

• **Specifies how long a session can be idle before being disconnected**

Complete the following steps to configure an SSH connection to your security appliance:

Step 189 Obtain an SSH client and install it on the system from which you want to establish the SSH connection.

Step 190 Use the **crypto key zeroize rsa** command to delete any previously created RSA keys.

Step 191 Use the **write memory** command to save the certificate authority (CA) state and complete the erasure of the old RSA key pair.

Step 192 Use the **domain-name** command to configure the domain name.

Step 193 Use the **crypto key generate rsa** command to generate an RSA key pair to use to encrypt SSH sessions.

Step 194 Use the **write memory** command to save the keys to Flash memory.

Step 195 Use the **ssh** command to specify the host or network authorized to initiate an SSH connection to the security appliance. Use the **no** keyword to remove this command from the configuration.

Step 196 Use the **ssh timeout** command to specify the duration in minutes that a session can be idle before being disconnected. The default duration is five minutes.

Note	The password used to perform local authentication is the same as the one used for Telnet access. The default for this password is cisco. To change it, use the **passwd** command.

The syntaxes for the **crypto key** commands are as follows:

```
crypto key zeroize {rsa | dsa} [label key-pair-label]
[default] [noconfirm]
crypto key generate rsa [usage-keys | general-keys] [label
key-pair-label] [modulus size] [noconfirm]
```

general-keys	Generates a single pair of general purpose keys. This is the default key-pair type.
label *key-pair-label*	Specifies the name to be associated with the key pair(s). This key pair must be uniquely labeled. If you attempt to create another key pair with the same label, the security appliance displays a warning message. If no label is provided when the key is generated, the key pair is statically named <Default-RSA-Key>.
modulus *size*	Specifies the modulus size of the key pair(s): 512, 768, 1024, and 2048. The default modulus size is 1024.
noconfirm	Suppresses all interactive prompting.
usage-keys	Generates two key pairs, one for signature use and one for encryption use. This implies that two certificates for the corresponding identity are required.
default	Removes RSA key pairs with no labels. This keyword is legal only with RSA key pairs.
dsa	Specifies Directory System Agent (DSA) as the key type.
rsa	Specifies RSA as the key type.

The syntax for the **domain-name** command is as follows:

```
domain-name name
```

name	The name of the domain.

The syntaxes for the **ssh** configuration commands are as follows:

```
ssh {ip_address mask | ipv6_address/prefix} interface
ssh timeout number
```

interface	The security appliance interface on which SSH is enabled. If not specified, SSH is enabled on all interfaces except the outside interface.
ip_address	IPv4 address of the host or network authorized to initiate an SSH connection to the security appliance. For hosts, you can also enter a host name.
ipv6_address/prefix	The IPv6 address and prefix of the host or network authorized to initiate an SSH connection to the security appliance.
mask	Network mask for *ip_address.*
number	Specifies the duration in minutes that an SSH session can remain inactive before being disconnected. Valid values are from 1 to 60 minutes.

Connecting to the Security Appliance with an SSH Client

Cisco.com

username: pix
password: telnetpassword

SSH

Internet
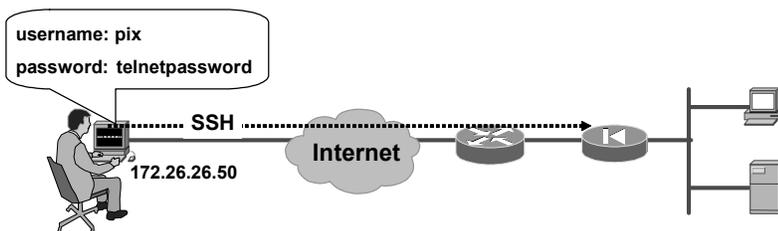
172.26.26.50

```
fw1(config)# crypto key zeroize rsa
fw1(config)# write memory
fw1(config)# domain-name cisco.com
fw1(config)# crypto key generate rsa modulus 1024
fw1(config)# write memory
fw1(config)# ssh 172.26.26.50 255.255.255.255 outside
fw1(config)# ssh timeout 30
```

SNPA v4.0—19-7

To establish an SSH connection to your security appliance console, enter the username **pix** and the Telnet password at the SSH client. When starting an SSH session, the security appliance displays a dot (.) on the console before the SSH user authentication prompt appears, as follows:

```
firewall(config)# .
```

The display of the dot does not affect the functionality of SSH. The dot appears at the console when generating a server key or decrypting a message using private keys during SSH key exchange before user authentication occurs. These tasks can take up to two minutes or longer. The dot is a progress indicator that verifies that the security appliance is busy and has not hung.

In the figure, an RSA key pair is generated for the security appliance using the default key modulus size of 1024. Host 172.26.26.50 is authorized to initiate an SSH connection to the security appliance.

Viewing, Disabling, and Debugging SSH

firewall#

```
show ssh sessions [ip_address]
```

- **Enables you to view the status of your SSH sessions**

firewall#

```
ssh disconnect session_id
```

- **Disconnects an SSH session**

firewall(config)#

```
clear configure ssh
```

- **Removes all SSH command statements from the configuration**

firewall(config)#

```
debug ssh
```

- **Enables SSH debugging**

SNPA v4.0—19-8

Use the **show ssh sessions** command to list all active SSH sessions on the security appliance. The **ssh disconnect** command enables you to disconnect a specific session.

The **show ssh sessions** command provides the following display:

```
Session ID      Client IP       Version Encryption      State Username
    0           172.16.25.15    1.5     3DES            4      -
    1           172.26.26.50    1.5     DES             6      pix
    2           172.16.25.11    1.5     3DES            4      -
```

The following are the different parts of the **show ssh sessions** command display:

- **Session ID column:** A unique number that identifies an SSH session.

- **Client IP column:** The IP address of the system running an SSH client.

- **Version column:** Lists the protocol version number that the SSH client supports.

- **Encryption column:** Lists the type of encryption that the SSH client is using.

- **State column:** Lists the progress the client is making as it interacts with the security appliance.

- **Username column:** Lists the login username that has been authenticated for the session. The "pix" username appears when authentication other than authentication, authorization, and accounting (AAA) is used.

Use the **clear configure ssh** command to remove all **ssh** command statements from the configuration, and use the **no ssh** command to remove selected **ssh** command statements. The **debug ssh** command displays information and error messages associated with the **ssh** command.

The syntaxes for these SSH commands are as follows:

```
show ssh sessions [ip_address]
ssh disconnect session_id
clear configure ssh
ssh debug
```

ip_address	The IP address of a system running an SSH client.
session_id	Identifier for the specific session that you want to disconnect.

Managing User Access Levels

This topic describes how to configure and use local user authentication and command authorization.

Command Authorization Overview

Cisco.com

The purpose of command authorization is to securely and efficiently administer the security appliance.

It has the following types:

- **Enable-level command authorization with passwords**
- **Command authorization using the local user database**
- **Command authorization using ACS**

SNPA v4.0—19-10

Command authorization is a way of facilitating and controlling administration of the security appliance. There are three types of command authorizations that can be used to control which users execute certain commands:

- Enable-level command authorization with passwords
- Command authorization using the local user database
- Command authorization using Access Control Server (ACS)

Enable-Level Command Authorization

Complete the following tasks to configure and use enable-level command authorization:

- **Use the** enable **command to create privilege levels and assign passwords to them.**
- **Use the** privilege **command to assign specific commands to privilege levels.**
- **Use the** aaa authorization **command to enable the command authorization feature.**
- **Use the** enable **command to access the desired privilege level.**

SNPA v4.0—19-11

The first type of command authorization, enable-level with passwords, allows you to use the **enable** command with the priv_level option to access a security appliance privilege level and then use any command assigned to that privilege level or to a lower privilege level. To configure this type of command authorization, you must create and password-protect your privilege levels, assign privilege levels to commands, and enable the command authorization feature.

Create and Password-Protect Your Privilege Levels

Cisco.com

```
fw1> enable 10
password: PasswOrD
```

10.0.0.11

Internet
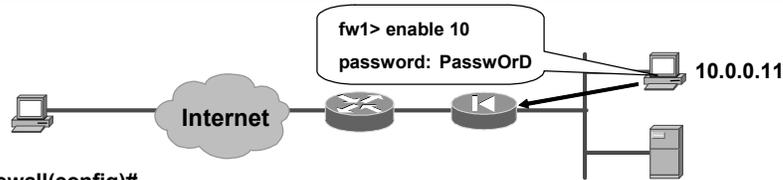
firewall(config)#

```
enable password password [level level] [encrypted]
```

- **Configures enable passwords for the various privilege levels**

```
fw1(config)# enable password Passw0rD level 10
```

firewall(config)#

```
enable [level]
```

- **Provides access to a particular privilege level from the > prompt**

```
fw1> enable 10
Password: Passw0rD
fw1#
```

SNPA v4.0—19-12

The security appliance supports up to sixteen privilege levels: levels zero through fifteen. You can create privilege levels and secure them by using the **enable password** command. You can then gain access to a particular privilege level from the > prompt by entering the **enable** command with a privilege level designation and entering the password for that level when prompted.

After you are inside a privilege level, you can execute the commands assigned to that level as well as commands assigned to lower privilege levels. For example, from privilege level 15, you can execute every command because this is the highest privilege level. If you do not specify a privilege level when entering enable mode, the default of 15 is used. Therefore, creating a strong password for level 15 is important.

The syntaxes for the **enable** commands when used with command authorization are as follows:

```
enable [1evel]
enable password password [level 1evel] [encrypted]
```

level *level*	(Optional) Sets a password for a privilege level between 0 and 15.
password	Sets the password as a case-sensitive string of up to 16 alphanumeric and special characters. You can use any character in the password except a question mark or a space.
encrypted	(Optional) Specifies that the password is in encrypted form. The password is saved in the configuration in encrypted form, so you cannot view the original password after you enter it. If for some reason you need to copy the password to another security appliance but do not know the original password, you can enter the **enable password** command with the encrypted password and this keyword. Normally, you only see this keyword when you enter the **show running-config enable** command.

Assign Commands to Privilege Levels and Enable Command Authorization

```
firewall> enable 10
Password: Passw0rD
firewall# config t
firewall(config)# access-list . . .
```

firewall(config)#

```
privilege [show | clear | configure] level level [mode
{enable | configure}] command command
```

• **Configures user-defined privilege levels for security appliance commands**

firewall(config)#

```
aaa authorization command {LOCAL | server-tag}
```

• **Enables command authorization**

```
fw1(config)# enable password Passw0rD level 10
fw1(config)# privilege show level 8 command access-list
fw1(config)# privilege configure level 10 command access-list
fw1(config)# aaa authorization command LOCAL
```

SNPA v4.0—19-13

To assign commands to privilege levels, use the **privilege** command. Replace the level argument with the privilege level, and replace the command argument with the command you want to assign to the specified level. You can use the **show**, **clear**, or **configure** parameter to optionally set the privilege level for the command modifiers of the specified command. The **privilege** command can be removed by using the **no** keyword.

In the figure, privilege levels are set for the different command modifiers of the **access-list** command. The first **privilege** command entry sets the privilege level of **show access-list** (the show modifier of command **access-list**) to 8. The second **privilege** command entry sets the privilege level of the configure modifier to 10. The **aaa authorization command LOCAL** command is then used to enable command authorization. The user knows the highest privilege level to which the **access-list** command is assigned and also knows the password for the level. The user is therefore able to view and create access control lists (ACLs) by entering level 10.

Use the **privilege** command without a show, clear, or configure parameter to set the privilege level for all the modifiers of the command. For example, to set the privilege level of all modifiers of the **access-list** command to a single privilege level of 10, enter the following command:

```
privilege level 10  command access-list
```

For commands that are available in multiple modes, use the **mode** parameter to specify the mode in which the privilege level applies. Do not use the mode parameter for commands that are not mode-specific.

The syntax of the **privilege** command is as follows:

```
privilege [show | clear | configure] level level [mode enable
| configure] command command
```

clear	(Optional) Sets the privilege level for the **clear** command corresponding to the command specified.
command *command*	Specifies the command on which to set the privilege level.
configure	(Optional) Sets the privilege level for the command specified.
level *level*	Specifies the privilege level; valid values are from 0 to 15.
mode enable	(Optional) Indicates that the level is for the enable mode of the command.
mode configure	(Optional) Indicates that the level is for the configure mode of the command.
show	(Optional) Sets the privilege level for the **show** command corresponding to the command specified.

The syntax for the **aaa authorization** command for use with command authorization is as follows:

```
aaa authorization command {LOCAL | server-tag}
```

LOCAL	Specifies the use of the security appliance local user database for local command authorization (using privilege levels). If **LOCAL** is specified after a TACACS+ server group tag, the local user database is used for command authorization only as a fallback when the TACACS+ server group is unavailable.
server-tag	Specifies a predefined server group tag for the TACACS+ authorization server. The AAA server group tag as defined by the **aaa-server** command. You can also enter **LOCAL** for the group tag value and use the local command authorization privilege levels.

Command Authorization Using the Local User Database

Complete the following tasks to configure and use command authorization with the local user database:

- **Use the** privilege **command to assign specific commands to privilege levels.**
- **Use the** username **command to create user accounts in the local user database and assign privilege levels to the accounts.**
- **Use the** aaa authorization **command to enable command authorization.**
- **Use the** aaa authentication **command to enable authentication using the local database.**
- **Use the** login **command to log in and access privilege levels.**

SNPA v4.0—19-14

A second way of controlling which commands users can execute is to configure command authorization using the local user database. After assigning commands to privilege levels with the **privilege** command, use the **username** command to define user accounts and their privilege levels in the local security appliance user database. You can define as many user accounts as you need. After defining the user accounts, enable command authorization with the **aaa authorization** command. To enable a direct username and password prompt, enable authentication via the local user database by entering the **aaa authentication enable console LOCAL** command.

Creating User Accounts in the Local Database
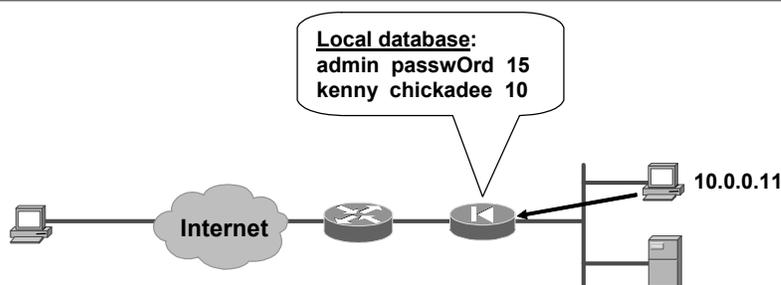
Local database:
admin passwOrd 15
kenny chickadee 10

Internet

10.0.0.11

firewall(config)#

```
username {name} {nopassword | password password [encrypted]}
  [privilege priv_level]}
```

• **Configures the username for the specified privilege level**

```
fw1(config)# username admin password passw0rd privilege 15
fw1(config)# username kenny password chickadee privilege 10
```

SNPA v4.0—19-15

Use the **username** command to create user accounts in the local user database. You can create a password for the user or you can use the **nopassword** keyword to create a user account with no password. Use the **encrypted** keyword if the password you are supplying is already encrypted, and use the **privilege** keyword to assign a privilege level to the user.

To delete an existing user account, use the **no username** command. To remove all the entries from the user database, enter the **clear configure username** command.

In the figure, the **username** command assigns a privilege level of 15 to the user account admin and a privilege level of 10 to the user account kenny.

The syntaxes for the **username** commands are as follows:

```
username {name} {nopassword | password password [encrypted]}
[privilege priv_level]}
no username [name]
clear configure username
```

name	Provides the name of the user.
nopassword	Indicates that this user needs no password.
password *password*	Indicates that this user has a password, and provides the password.
encrypted	Indicates that the password is encrypted.
privilege *priv_level*	Sets a privilege level for this user. The range is from 0 to 15, with lower numbers having less ability to use commands and administer the security appliance. The default privilege level is 2. The typical privilege level for a system administrator is 15.

Configuring Authentication with the Local Database

```
firewall> login
Username: kenny
Password: chickadee
firewall# config t
firewall(config)# access-list . . .
```

10.0.0.11

Internet

firewall(config)#

```
aaa authentication {serial | enable | telnet | ssh | http}
console server-tag [LOCAL]
```

```
fw1(config)# privilege configure level 10 command access-list
fw1(config)# username kenny password chickadee privilege 10
fw1(config)# aaa authorization command LOCAL
fw1(config)# aaa authentication enable console LOCAL
```
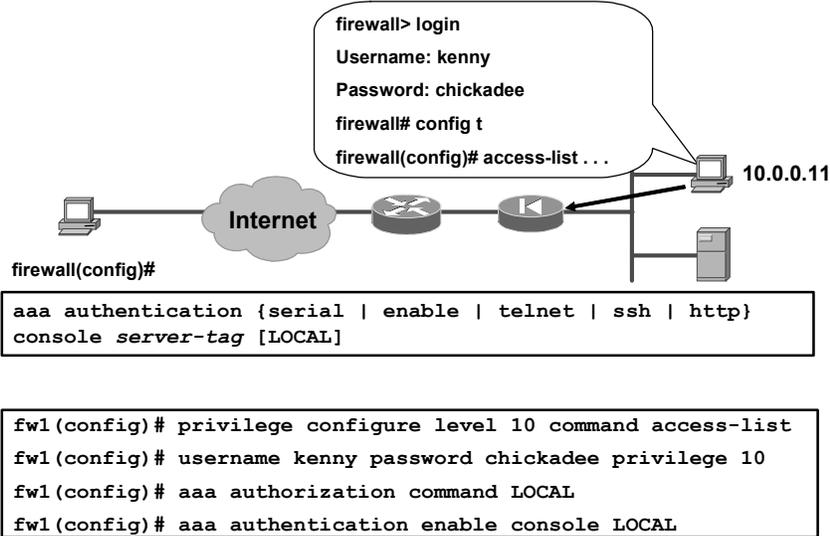
SNPA v4.0—19-16

After you enter the **aaa authentication enable console LOCAL** command, the console prompts for a username and password when you execute the **enable** or **login** command. You can log in to the security appliance using the LOCAL internal user database. After you enter the **aaa authentication enable console LOCAL** command, you are no longer able to access the security appliance using the **enable** command with the priv_level option.

When users log in to the security appliance, they can enter any command assigned to their privilege level or to lower privilege levels. For example, a user account with a privilege level of 15 can access every command because this is the highest privilege level. A user account with a privilege level of 0 can only access the commands assigned to level 0.

The syntax for the **aaa authentication** command used with command authorization is as follows:

```
aaa authentication [serial | enable | telnet | ssh | http]
console server-tag [LOCAL]
```

serial	Enables or disables authentication of admin sessions established on the serial interface to the console. Valid server group protocols are LOCAL, Remote Authentication Dial-In User Service (RADIUS), and Terminal Access Controller Access Control System Plus (TACACS+).
enable	Enables or disables authentication on entry to privileged mode. Valid server group protocols are LOCAL, RADIUS, and TACACS+.
telnet	Enables or disables authentication of admin sessions over Telnet. Valid server group protocols are LOCAL, RADIUS, and TACACS+.
ssh	Enables or disables authentication of admin sessions over SSH. Valid server group protocols are LOCAL, RADIUS, and TACACS+.

http	Enables or disables authentication of admin sessions over HTTP. Valid server group protocols are LOCAL, RADIUS, and TACACS+.
console	Specifies that access to the console requires authentication.
server-tag	The AAA server group tag defined by the **aaa-server** command.
	For cut-through proxy and "to the box" authentication, you can also use the local security appliance user authentication database by specifying the server group tag **LOCAL**. If **LOCAL** is specified for server-tag and the local user credential database is empty, the following warning message appears:
	``` Warning:local database is empty! Use 'username' command to define local users. ```
	Conversely, if the local database becomes empty when **LOCAL** is still present in the command, the following warning message appears:
	``` Warning:Local user database is empty and there are still commands using 'LOCAL' for authentication. ```
LOCAL	The keyword **LOCAL** has two uses. It can designate the use of a local authentication server, or it can specify fallback to the local database if the designated authentication server is unavailable.

Note The **logout** command logs you out of the currently logged in user account.

Command Authorization Using ACS

Complete the following tasks to configure and use ACS command authorization:

- **Create a user profile on the TACACS+ server with all the commands that the user is permitted to execute.**
- **Use the** aaa-server **command to specify the TACACS+ server.**
- **Use the** aaa authentication **command to enable authentication with a TACACS+ server.**
- **Use the** aaa authorization **command to enable command authorization with a TACACS+ server.**

Only enable authorization with ACS if you are absolutely sure that you have fulfilled the following requirements:

- You have created entries for enable_1, enable_15, and any other levels to which you have assigned commands.

- If you are enabling authentication with usernames:

    — You have a user profile on the TACACS+ server with all the commands that the user is permitted to execute.

    — You have tested authentication with the TACACS+ server.

- You are logged in as a user with the necessary privileges.

- Your TACACS+ system is completely stable and reliable. The necessary level of reliability typically requires that you have a fully redundant TACACS+ server system and fully redundant connectivity to the security appliance.

When configuring the command authorization feature, do not save your configuration until you are sure it works the way you want. If you get locked out of your security appliance, you can usually recover access by simply reloading it.

aaa authorization Command for Command Authorization with ACS
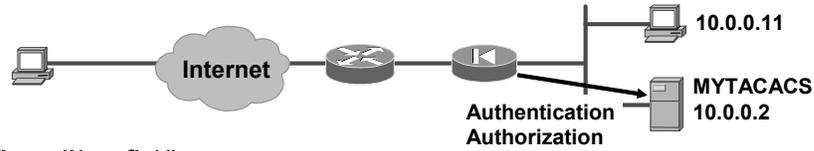
```
firewall(config)#

aaa authorization command {LOCAL | server-tag}
```

```
fw1(config)# aaa-server MYTACACS protocol tacacs+
fw1(config-aaa-server-group)# aaa-server MYTACACS
  (inside) host 10.0.0.2 thekey timeout 20
fw1(config-aaa-server-host)# aaa authentication enable
  console MYTACACS
fw1(config)# aaa authorization command MYTACACS
```

Use the **aaa authorization** command to enable command authorization with a TACACS+ server. You must also use the **aaa-server** command to create the *server-tag*.

The syntax for the **aaa authorization command**, when used to configure command authorization using ACS, is as follows:

```
aaa authorization command {LOCAL | server-tag}
```

LOCAL	Specify the use of the security appliance local user database for local command authorization (using privilege levels). If **LOCAL** is specified after a TACACS+ server group tag, the local user database is used for command authorization only as a fallback when the TACACS+ server group is unavailable.
server-tag	Specify a predefined server group tag for the TACACS+ authorization server. The AAA server group tag as defined by the **aaa-server** command. You can also enter **LOCAL** for the group tag value and use the local command authorization privilege levels.

Viewing Your Command Authorization Configuration

Cisco.com
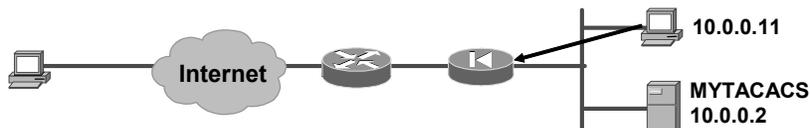
```
firewall#
show running-config [all] privilege [all | command
command | level level]
```

```
firewall#
show curpriv
```
• **Displays the user account that is currently logged in**

SNPA v4.0—19-19

To view the command assignments for each privilege level, use the **show running-config privilege all** command. The system displays the current assignment of each command-line interface (CLI) command to a privilege level. The following example illustrates the first part of the display:

```
fw(config)# show running-config privilege all
privilege show level 15 command aaa
privilege clear level 15 command aaa
privilege configure level 15 command aaa
privilege show level 15 command aaa-server
privilege clear level 15 command aaa-server
privilege configure level 15 command aaa-server
privilege show level 15 command access-group
privilege clear level 15 command access-group
privilege configure level 15 command access-group
privilege show level 15 command access-list
privilege clear level 15 command access-list
privilege configure level 15 command access-list
privilege show level 15 command activation-key
privilege configure level 15 command activation-key
```

Use the **show running-config privilege level** command with the level option to display the command assignments for a specific privilege level. Use the **show running-config privilege command** command to display the privilege level assignment of a specific command.

To view the user account that is currently logged in, enter the **show curpriv** command. The system displays the current username and privilege level, as follows:

```
fw(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV P_CONF
fw(config)# exit
fw(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV
fw(config)# exit
fw(config)# show curpriv
Username : enable_1
Current privilege level : 1
Current Mode/s : P_UNPR
```

The username indicates the name that the user entered when the user logged in, P_PRIV indicates that the user has entered the **enable** command, and P_CONF indicates that the user has entered the **config terminal** command.

The syntaxes for the **show** commands are as follows:

```
show running-config  privilege [all | command command | level
level]
show curpriv
```

all	(Optional) First occurrence—Displays the default privilege level.
all	(Optional) Second occurrence—Displays the privilege level for all commands.
command *command*	(Optional) Displays the privilege level for a specific command.
level *level*	(Optional) Displays the commands that are configured with the specified level; valid values are from 0 to 15.

Lockout

Local database:
admin passwOrd 15
kenny chickadee 10

Internet

10.0.0.11

MYTACACS
10.0.0.2
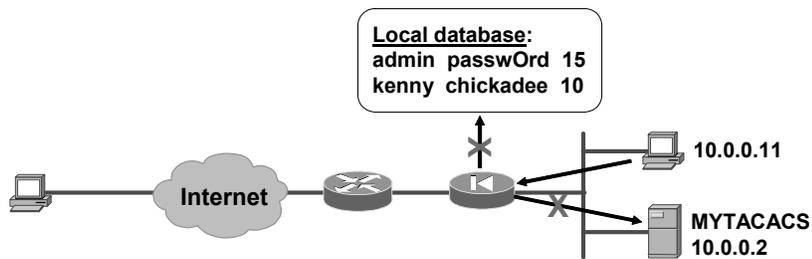
SNPA v4.0—19-20

When you are configuring the command authorization feature, do not save your configuration until you are sure it works the way you want. If you get locked out of your security appliance, you can usually recover access by simply reloading it. If you have already saved your configuration and you find that you configured authentication using the LOCAL database but did not configure any usernames, you created a lockout problem. You can also encounter a lockout problem by configuring command authorization using a TACACS+ server if the TACACS+ server is unavailable, down, or misconfigured.

If you cannot recover access to the security appliance by restarting your PIX Security Appliance, use your web browser to access the following website: http://www.cisco.com/warp/customer/110/34.shtml

This website provides a downloadable file with instructions for using it to remove the lines in the PIX Security Appliance configuration that enable authentication and cause the lockout problem. If there are Telnet or console **aaa authentication** commands in PIX Security Appliance Software v6.2 or v6.3, the system will also prompt to remove them.

Note	If you have configured AAA on the PIX Security Appliance, and the AAA server is down, you can access the PIX Security Appliance by entering the Telnet password initially, and then **pix** as the username and the enable password (**password**). If there is no enable password in the PIX Security Appliance configuration, enter **pix** for the username and press **ENTER**. If the enable and Telnet passwords are set but not known, you will need to continue with the password recovery process.

The PIX Password Lockout utility is based on the PIX Security Appliance software version you are running. Use one of the following files, depending on the PIX Security Appliance software version you are running:

- np70.bin (7.0 version)
- np63.bin (6.3 version)
- np62.bin (6.2 version)
- np61.bin (6.1 version)
- np60.bin (6.0 version)
- np53.bin (5.3 version)
- np52.bin (5.2 version)
- np51.bin (5.1 version)

You can encounter a different type of lockout problem if you use the **aaa authorization** command and *server-tag* argument, and you are not logged in as the correct user. For every command you enter, the PIX Security Appliance displays the following message:

```
Command Authorization failed
```

This occurs because the TACACS+ server does not have a user profile for the user account that you used for logging in. To prevent this problem, make sure that the TACACS+ server has all the users configured with the commands that they can execute. Also make sure that you are logged in as a user with the required profile on the TACACS+ server.

Password Recovery PIX

- **Download the following file from Cisco.com: npXX.bin (where XX = the PIX Firewall image version number).**
- **Reboot the system and break the boot process when prompted to go into monitor mode.**
- **Set the interface, IP address, gateway, server, and file to TFTP the previously downloaded image.**
- **Follow the directions displayed.**

Password recovery for the PIX Security Appliance versions through 7.0 requires a TFTP server. To perform a password recovery using Trivial File Transfer Protocol (TFTP), complete the following steps:

Step 197 Download the PIX Security Appliance password tool from Cisco.com to a TFTP server accessible from the security appliance.

Step 198 Connect to the security appliance console port.

Step 199 Power off the security appliance, and then power it on.

Step 200 Immediately after the startup messages appear, press the **Escape** key to enter monitor mode.

Step 201 Configure the network settings for the interface that accesses the TFTP server by entering the following commands:

```
monitor> interface interface_id
monitor> address interface_ip
monitor> server tftp_ip
monitor> file pw_tool_name
monitor> gateway gateway_ip
```

Step 202 Download the PIX Security Appliance password tool from the TFTP server by entering the following command:

```
monitor> tftp
```

Note If you have trouble reaching the server, you can enter the **ping** *address* command to test the connection.

Step 203   At the "Do you wish to erase the passwords?" prompt, enter **Y**.

You can now log in with the default login password of "cisco" and the blank enable password.

On the PIX 500 Series Security Appliance, the **no service password-recovery** command forces the PIX Security Appliance password tool to prompt the user to erase all Flash file systems. The user cannot use the PIX Security Appliance password tool without first performing this erasure. If a user chooses not to erase the Flash file system, the security appliance reloads. Because password recovery depends on maintaining the existing configuration, this erasure prevents you from recovering a password. However, disabling password recovery prevents unauthorized users from viewing the configuration or inserting different passwords. In this case, to recover the system to an operating state, load a new image and a backup configuration file, if available.

Password Recovery ASA

Cisco.com

Internet

192.168.0.0

Password? — 10.0.0.11

10.0.0.3
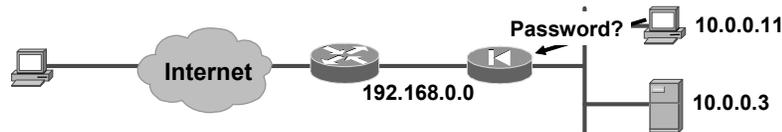
firewall(config)#

```
service password-recovery
```

- **Enables password recovery**
- **On by default**

```
fw1(config)# no service password-recovery
WARNING: Executing "no service password-recovery" has
  disabled the password recovery mechanism and disabled
  access to ROMMON. The only means of recovering from
  lost or forgotten passwords will be for ROMMON to
  erase all file systems including configuration files
  and images. You should make a backup of your
  configuration and have a mechanism to restore images
  from the ROMMON command line.
```

SNPA v4.0—19-22

On the ASA, if you forget the passwords, you can boot the security appliance into ROMMON by pressing the **Escape** key on the terminal keyboard when prompted during startup. Then set the security appliance to ignore the startup configuration by changing the configuration register (see the **config-register** command). For example, if your configuration register is the default 0x1, then change the value to 0x41 by entering the **confreg 0x41** command. After reloading the security appliance, it loads a default configuration, and you can enter privileged EXEC mode using the default passwords. Then load the startup configuration by copying it to the running configuration and reset the passwords. Finally, set the security appliance to boot as before by setting the configuration register to the original setting. For example, enter the **config-register 0x1** command in global configuration mode.

On the ASA, the **no** version of the **service password-recovery** command prevents a user from entering ROMMON with the configuration intact. When a user enters ROMMON, the security appliance prompts the user to erase all Flash file systems. The user cannot enter ROMMON without first performing this erasure. If a user chooses not to erase the Flash file system, the security appliance reloads. Because password recovery depends on using ROMMON and maintaining the existing configuration, this erasure prevents you from recovering a password. However, disabling password recovery prevents unauthorized users from viewing the configuration or inserting different passwords. In this case, to recover the system to an operating state, load a new image and a backup configuration file, if available. The **service password-recovery** command appears in the configuration file for informational purposes only; when you enter the command at the CLI prompt, the setting is saved in non-volatile random-access memory (NVRAM). The only way to change the setting is to enter the command at the CLI prompt. Loading a new configuration with a different version of the command does not change the setting. If you disable password recovery when the security appliance is configured to ignore the startup configuration at startup (in preparation for password recovery), the security appliance changes the setting to boot the startup configuration as usual. If you use failover, and the standby unit is configured to ignore the startup configuration, the same change is made to the configuration register when the **no service password recovery** command replicates to the standby unit.

The following example shows when to enter ROMMON at startup and how to complete a password recovery operation:

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.
Use ? for help.
rommon #0> confreg
Current Configuration Register: 0x00000001
Configuration Summary:
boot default image from Flash
Do you wish to change this configuration? y/n [n]: n
rommon #1> confreg 0x41
Update Config Register (0x41) in NVRAM...
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.
Loading disk0:/ASA_7.0.bin... Booting...
###################
...
Ignoring startup configuration as instructed by configuration
register.
Type help or '?' for a list of available commands.
hostname> enable
Password:
hostname# configure terminal
hostname(config)# copy startup-config running-config
Destination filename [running-config]?
Cryptochecksum(unchanged): 7708b94c e0e3f0d5 c94dde05 594fbee9
892 bytes copied in 6.300 secs (148 bytes/sec)
hostname(config)# enable password NewPassword
hostname(config)# config-register 0x1
```

Managing Software, Licenses, and Configurations

This topic describes how to manage software, licenses, and configuration files on the security appliance.

Viewing Directory Contents

firewall(config)#

```
dir [/all] [all-filesystems] [/recursive] [disk0: |
disk1: | flash: | system:] [path]
```

- Displays the directory contents.
- The pwd command displays the current working directory.

```
fw1# dir
Directory of disk:/
8 -rw- 5124096 13:01:10 Apr 19 2005  pix701.bin
9 -rw- 4908    12:52:39 Mar 16 2005  old_running2.cfg
10-rw- 4087    10:03:57 Apr 04 2005  old_running.cfg
15998976 bytes total (5573632 bytes free)
```

SNPA v4.0—19-24

Use the **dir** command to display the directory contents. The **dir** command without keywords or arguments displays the directory contents of the current directory.

The syntax for the **dir** command is as follows:

```
dir [/all] [all-filesystems] [/recursive] [disk0: | disk1: |
flash: | system:] [path]
```

/all	(Optional) Displays all files.
all-filesystems	(Optional) Displays the files of all filesystems.
disk0:	(Optional) Specifies the internal Flash memory, followed by a colon.
disk1:	(Optional) Specifies the external Flash memory card, followed by a colon.
/recursive	(Optional) Displays the directory contents recursively.
system:	(Optional) Displays the directory contents of the file system.
flash:	(Optional) Displays the directory contents of the default Flash partition.
path	(Optional) Specifies a specific path.

Viewing File Contents

more → 10.0.0.11

Internet 192.168.0.0 10.0.0.3

firewall#

```
more {/ascii | /binary| /ebcdic | disk0: |
disk1: | flash: | ftp: | http: | https: |
system: | tftp:}filename
```

- **Displays the contents of a file.**

```
fw1# more test.cfg
: Saved
: Written by enable_15 at 10:04:01 Apr 14 2005
XXX Version X.X(X)
nameif vlan300 outside security10
enable password 8Ry2YjIyt7RRXU24 encrypted
...
```

SNPA v4.0—19-25

Use the **more** command to display the contents of a file.

The syntax for the **more** command is as follows:

```
more {/ascii | /binary| /ebcdic | disk0: | disk1: | flash: |
ftp: | http: | https: | system: | tftp:}filename
```

/ascii	(Optional) Displays a binary file in binary mode and an ASCII file in binary mode.
/binary	(Optional) Displays any file in binary mode.
/ebcdic	(Optional) Displays binary files in extended binary coded decimal interchange code (EBCDIC).
disk0:	(Optional) Displays a file on the internal Flash memory.
disk1:	(Optional) Displays a file on the external Flash memory card.
flash:	(Optional) Specifies the internal Flash memory, followed by a colon. In the ASA 5500 series, the **flash** keyword is aliased to **disk0**.
ftp:	(Optional) Displays a file on an FTP server.
http:	(Optional) Displays a file on a website.
https:	(Optional) Displays a file on a secure website.
system:	(Optional) Displays the file system.
tftp:	(Optional) Displays a file on a TFTP server.
filename	Specifies the name of the file to display.

Directory Management

```
firewall#
mkdir [/noconfirm] [disk0: | disk1: | flash:]path
```
   • **Creates a new directory**

```
firewall#
rmdir [/noconfirm] [disk0: | disk1: | flash:]path
```
   • **Removes a directory**

```
firewall#
cd [disk0: | disk1: | flash:] [path]
```
   • **Changes the current working directory to the one specified.**

SNPA v4.0—19-26

Use the **mkdir** command to create a new directory. If a directory with the same name already exists, the new directory is not created. To remove the existing directory, use the **rmdir** command. If the directory is not empty, the **rmdir** command fails. Use the **cd** command to change the current working directory to the one specified. If you do not specify a directory, the directory is changed to the root directory.

The syntax for the **mkdir, rmdir**, and **cd** commands is as follows:

```
mkdir [/noconfirm] [disk0: | disk1: | flash:]path
rmdir [/noconfirm] [disk0: | disk1: | flash:]path
cd [disk0: | disk1: | flash:] [path]
```

noconfirm	(Optional) Suppresses the confirmation prompt.
disk0:	(Optional) Specifies the internal Flash memory, followed by a colon.
disk1:	(Optional) Specifies the external Flash memory card, followed by a colon.
flash:	(Optional) Specifies the internal Flash memory, followed by a colon. In the ASA 5500 series, the **flash** keyword is aliased to **disk0**.
path	The name and path of the directory to create.

Copying Files

Internet

192.168.0.0

copy

10.0.0.11

10.0.0.3
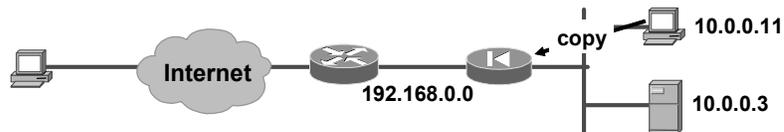
firewall(config)#

```
copy [/options] {url | local:[path] | running-config |
startup-config} {running-config | startup-config | url |
local:[path]}
```

- **Copies a file from one location to another**

```
fw1(config)# copy disk0:my_context/my_context.cfg
  startup-config
fw1(config)# copy disk0:my_context/my_context.cfg
  running-config
```

Use the **copy** command to copy a file from one location to another.

The syntax for the **copy** command is as follows:

```
copy [/options] {url | local:[path] | running-config |
startup-config} {running-config | startup-config | url |
local:[path]}
```

/options	Options used for the **copy** command: ■ **noconfirm**—Copies the file without a confirmation prompt. ■ **pcap**—Specifies the defaults of the preconfigured TFTP server.

url	Sets the context configuration URL All remote URLs must be accessible from the admin context. The options are as follows:
	
	■ **disk0:**/[path/]filename
	  — This option is only available for the ASA platform, and indicates the internal Flash memory. You can also use **flash** instead of **disk0**; they are aliased.
	
	■ **disk1:**/[*path*/]*filename*
	  — This option is only available for the ASA platform, and indicates the external Flash memory card.
	
	■ **flash:**/[*path*/]*filename*
	  — This option indicates the internal Flash card. For the ASA platform, **flash** is an alias for **disk0**.
	
	■ **ftp://**[*user***[:***password***]@**]*server*[:*port*]/[*path*/]*filename***[;type=***x*x]
	
	The **type** can be one of the following keywords:
	  — **ap**—ASCII passive mode
	  — **an**—ASCII normal mode
	  — **ip**—(Default) Binary passive mode
	  — **in**—Binary normal mode
	
	■ **http[s]://**[user[:password]@]server[:port]/[path/]filename
	
	■ **tftp://**[*use*r[:*password***]@**]*serve*r[:*por*t]/[*pa*th/]*filename***[;int=***interface_nam*e]
	  — Specifies the interface name if you want to override the route to the server address.

path	Path name that indicates the last component of the path to the file on the server.

Installing Application or ASDM Software Example

Internet
192.168.0.0
ASDM
10.0.0.11
10.0.0.3
TFTP server
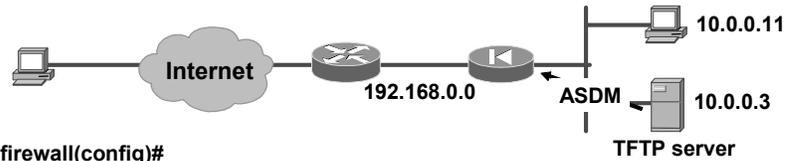
firewall(config)#

```
copy tftp://server[/path]/filename flash:/filename
```

- When you log into the security appliance during normal operation, you can copy the application software or ASDM software to the Flash file system from a TFTP, FTP, HTTP, or HTTPS server.

```
fw1(config)# copy tftp://10.0.0.3/cisco/123file.bin
  flash:/123file.bin
```

SNPA v4.0—19-28

When you install the ASA software, the existing activation key is extracted from the original image and stored in a file in the security appliance file system. On systems that support removable flash media, you can copy image and configuration files from one Flash device to another. Image, configuration, and ASDM files can be installed in either internal or removable media, or both. Images stored on removable media are not booted by default, unless the **boot system** command exists in the startup configuration and points to that image.

When you log in to the security appliance during normal operation, you can copy the application software or ASDM software to the Flash file system from a TFTP, FTP, HTTP, or Hypertext Transfer Protocol secure (HTTPS) server. For multiple context mode, you must be in the system execution space. Make sure that you have network access to the server, as follows:

- For single context mode, configure any interface, its IP address, and any static routes required to reach the server.

- For multiple context mode, you must first add the admin context and configure interfaces, IP addresses, and routing to provide network access.

Downloading and Backing Up Configuration Files Example

10.0.0.11

Internet

192.168.0.0

config

10.0.0.3

FTP server

firewall(config)#

```
copy ftp://[user[:password]@]server[/path]
/filename[;type=xx] startup-config
```

• **Copies the configuration file from an FTP server**

firewall(config)#

```
fw1# copy {startup-config | running-config |
disk0:[path/]filename}
ftp://[user[:password]@]server[/path]/filename[;type=xx]
```

• **Copies the configuration file to an FTP server**

```
fw1(config)# copy
  ftp://admin:letmein@10.0.0.3/configs/startup.cfg;type=an
  startup-config
```

In single context mode, or from the system configuration in multiple mode, you can copy the startup configuration, running configuration, or a configuration file by name on disk (such as the admin.cfg).

Image Upgrade and Activation Keys

This topic describes how to upgrade an image and an activation key.

Viewing Version Information

Cisco.com

version? 10.0.0.11

10.0.0.3

Internet

firewall(config)#

```
show version
```

- Displays the software version, hardware configuration, license key, and related uptime data

```
fw1# show version
…
This machine has a Restricted (R) license.
Serial Number: 12345678
Running Activation Key: 0xbd27f269 0xbc7ebd46
  0x1c73e474 0xbb782818 0x071dd0a6
Configuration has not been modified since last system
  restart.
```

SNPA v4.0—19-31

The **show version** command allows you to display the software version, operating time since the last reboot, processor type, Flash partition type, interface boards, serial number (BIOS ID), activation key value, license type (restricted [R] or unrestricted [UR]), and time stamp for when the configuration was last modified. The serial number listed with the **show version** command is for the Flash partition BIOS. This number is different from the serial number on the chassis. When you get a software upgrade, you will need the serial number that appears in the **show version** command, not the chassis number.

Image Upgrade

10.0.0.11

Internet   TFTP   10.0.0.3
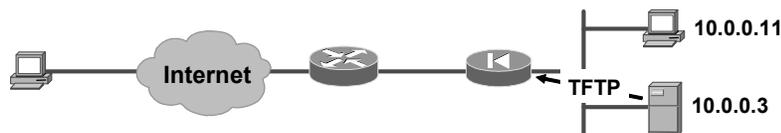
firewall(config)#

```
copy tftp://server[/path]/filename flash:/filename
```

- **Enables you to change software images without accessing the TFTP monitor mode.**

```
fw1# copy tftp://10.0.0.3/pix700.bin flash
```

- **The TFTP server at IP address 10.0.0.3 receives the command and determines the actual file location from its root directory information. The server then downloads the TFTP image to the security appliance.**

SNPA v4.0—19-32

The **copy tftp flash** command enables you to change software images without accessing the TFTP monitor mode. You can use this command to download a software image via TFTP with any PIX Security Appliance model running Version 5.1 or later. The image you download is made available to the security appliance on the next reload.

Be sure to configure your TFTP server to point to the image you wish to download. For example, to download the pix701.bin file from the D: partition on a Windows system whose IP address is 10.0.0.3, you would access the Cisco TFTP Server **View > Options** menu and enter the filename path in the TFTP server root directory edit box (for example, D:\pix_images). Copy the file to the security appliance, using the following command: **copy tftp://10.0.0.3/pix701.bin flash**.

The TFTP server receives the command and determines the actual file location from its root directory information. The server then downloads the TFTP image to the security appliance.
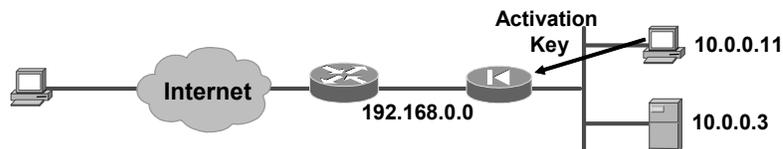

Note   Your TFTP server must be open when you enter the **copy tftp** command on the security appliance.

Entering a New Activation Key

Cisco.com

Activation Key

10.0.0.11

Internet

192.168.0.0

10.0.0.3

firewall(config)#

```
activation-key [activation-key-four-tuple| activation-
key-five-tuple]
```

• **Updates the activation key on your security appliance**
• **Used to enable licensed features on security appliance**

```
fw1(config)# activation-key 0x12345678 0xabcdef01
  0x2345678ab 0xcdef01234
```

SNPA v4.0—19-33

You can upgrade the license for your security appliance from the CLI. Before entering the activation key, ensure that the image in Flash and the running image are the same. You can do this by rebooting the security appliance before entering the new activation key. You will also need to reboot the security appliance after entering the new activation key for the change to take effect.

Enter the *activation-key-four-tuple* as a four-element hexadecimal string with one space between each element, or *activation-key-five-tuple* as a five-element hexidecimal string with one space between each element as follows:

```
0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e
```

The leading 0x specifier is optional; all values are assumed to be hexadecimal. The key is not stored in the configuration file. The key is tied to the serial number.

Use the **activation-key** command to enter an activation key. In this command, replace *activation-key-four-tuple* with the activation key you obtained with your new license as follows:

```
activation-key 0x12345678 0xabcdef01 0x2345678ab 0xcdef01234
```

The syntax for the **activation-key** command is as follows:

```
activation-key [activation-key-four-tuple| activation-key-
five-tuple]
```

activation-key-four-tuple	The activation key you obtained with your new license.
activation-key-five-tuple	The activation key you obtained with your new license.

Reload the security appliance to activate the Flash activation key.

Upgrading the Image and the Activation Key

Complete the following steps to upgrade the image and the activation key at the same time:

- **Step 1: Install the new image.**
- **Step 2: Reboot the system.**
- **Step 3: Update the activation key.**
- **Step 4: Reboot the system.**

If you are upgrading the image to a newer version and the activation key is also being changed, reboot the system twice, as follows:

Step 204 Install the new image.

Step 205 Reboot the system.

Step 206 Update the activation key.

Step 207 Reboot the system.

After the key update is complete, the system is reloaded a second time so that the updated licensing scheme can take effect.

If you are downgrading an image, you only need to reboot once, after installing the new image. In this situation, the old key is both verified and changed with the current image.

Troubleshooting the Activation Key Upgrade

Message	Problem and Resolution
The activation key you entered is the same as the running key.	Either the activation key has already been upgraded or you need to enter a different key.
The Flash image and the running image differ.	Reboot the security appliance and reenter the activation key.
The activation key is not valid.	Either you made a mistake entering the activation key or you need to obtain a valid activation key.

To view your current activation key, enter the **show activation-key** command. The following examples show the output from this command under different circumstances.

```
firewall(config)# show activation-key

Serial Number: 12345678 (0xbc614e)
Running activation key: 0xe02888da 0x4ba7bed6 0xf1c123ae
0xffd8624e

Licensed Features:
Maximum Physical Interfaces : 6
Maximum VLANs               : 25
Inside Hosts                : Unlimited
Failover                    : Active/Active
VPN-DES                     : Enabled
VPN-3DES-AES                : Enabled
Cut-through Proxy           : Enabled
Guards                      : Enabled
URL Filtering               : Enabled
Security Contexts           : 5
GTP/GPRS                    : Disabled
VPN Peers                   : Unlimited
This platform has an Unrestricted (UR) license.
The flash activation key is the SAME as the running key.
firewall(config)# show activation-key

Serial Number: 12345678 (0xbc614e)

Running activation key: 0xe02888da 0x4ba7bed6 0xf1c123ae
0xffd8624e
```

```
Licensed Features:
Maximum Physical Interfaces : 6
Maximum VLANs               : 25
Inside Hosts                : Unlimited
Failover                    : Active/Active
VPN-DES                     : Enabled
VPN-3DES-AES                : Enabled
Cut-through Proxy           : Enabled
Guards                      : Enabled
URL Filtering               : Enabled
Security Contexts           : 5
GTP/GPRS                    : Disabled
VPN Peers                   : Unlimited


Flash activation key: 0xe02388da 0x5ca7bed2 0xf1c123ae
0xffd8624t
Licensed Features:
Maximum Physical Interfaces : 6
Maximum VLANs               : 25
Inside Hosts                : Unlimited
Failover                    : Active/Active
VPN-DES                     : Enabled
VPN-3DES-AES                : Enabled
Cut-through Proxy           : Enabled
Guards                      : Enabled
URL Filtering               : Enabled
Security Contexts           : 5
GTP/GPRS                    : Disabled
VPN Peers                   : Unlimited


The flash activation key is DIFFERENT than the running key.
The flash activation key takes effect after the next reload.
firewall(config)# show activation-key


Serial Number: 12345678 (0xbc614e)


Running activation key: 0xe02888da 0x4ba7bed6 0xf1c123ae
0xffd8624e
Maximum Physical Interfaces : 6
Maximum VLANs               : 25
Inside Hosts                : Unlimited
Failover                    : Active/Active
VPN-DES                     : Enabled
VPN-3DES-AES                : Enabled
Cut-through Proxy           : Enabled
Guards                      : Enabled
URL Filtering               : Enabled
Security Contexts           : 5
GTP/GPRS                    : Disabled
```

```
VPN Peers                     : Unlimited
This platform has an Unrestricted (UR) license.


The flash image is DIFFERENT than the running image.
The two images must be the same in order to examine the flash
activation key.
```

Summary

This topic summarizes the key points discussed in this lesson.

Summary

- **SSH provides secure remote management of the security appliance.**
- **TFTP is used to upgrade the software image on security appliances.**
- **You can configure three different types of command authorization: enable level with password, local command authorization, and ACS command authorization.**
- **The security appliance can be configured to permit multiple users to access its console simultaneously via Telnet.**
- **You can enable Telnet to the security appliance on all interfaces.**
- **Password recovery for the security appliance requires a TFTP server.**

SNPA v4.0—19-36

Appendix 1

Configuring PIX Security Appliance Remote Access Using Cisco Easy VPN

Overview

This appendix describes how to configure Cisco Easy Virtual Private Network (VPN) Remote on the Cisco PIX Security Appliance 501 and PIX Security Appliance 506/506E hardware clients, using PIX Security Appliance Software v6.3. An overview of the PIX Security Appliance Easy VPN Remote feature is provided along with basic commands that are useful for configuring Easy VPN Remote. The appendix also explains how the PIX Security Appliance works with Point-to-Point Protocol over Ethernet, and describes the configuration steps. The appendix concludes with an explanation about how to configure the PIX Security Appliance Dynamic Host Configuration Protocol (DHCP) server on the PIX Security Appliance 501 or PIX Security Appliance 506/506E.

Objectives

Upon completing this appendix, you will be able to configure Cisco Easy VPN Remote on the PIX Security Appliance 501 and PIX Security Appliance 506/506E. This ability includes being able to meet these objectives:

- Describe the two Easy VPN modes of operation
- Configure the PIX Security Appliance as an Easy VPN Remote client
- Describe the PIX Security Appliance DHCP server feature
- Configure the PIX Security Appliance as a DHCP server
- Configure the PIX Security Appliance PPPoE client

PIX Security Appliance Easy VPN Remote Feature Overview

This topic describes the PIX Security Appliance Easy VPN Remote feature.

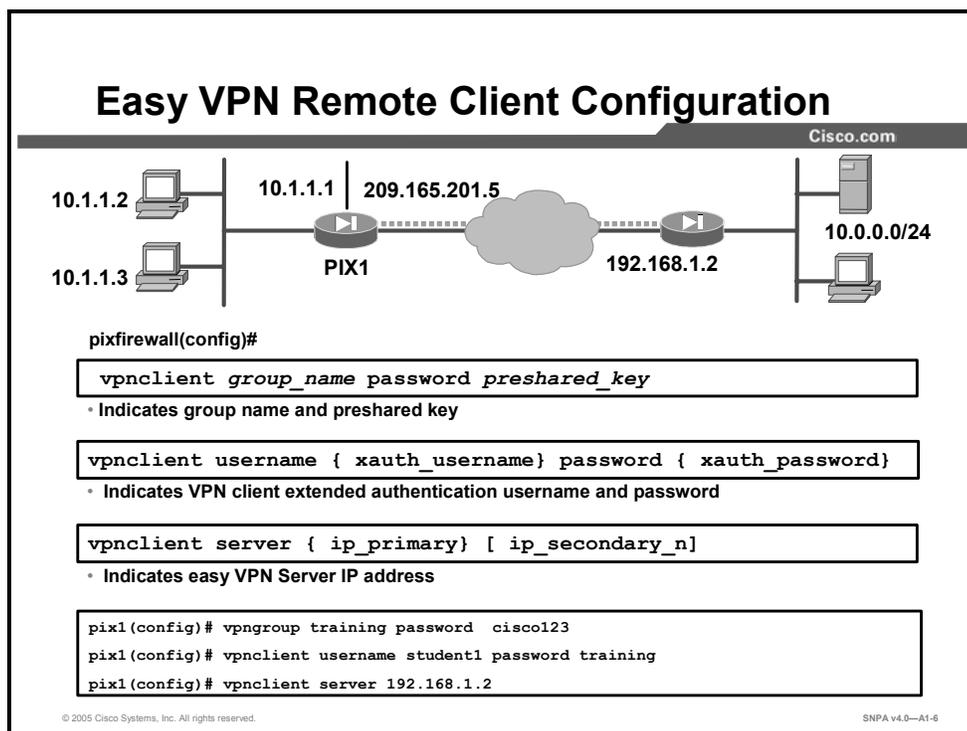## Implementing PIX Firewall Easy VPN Remote
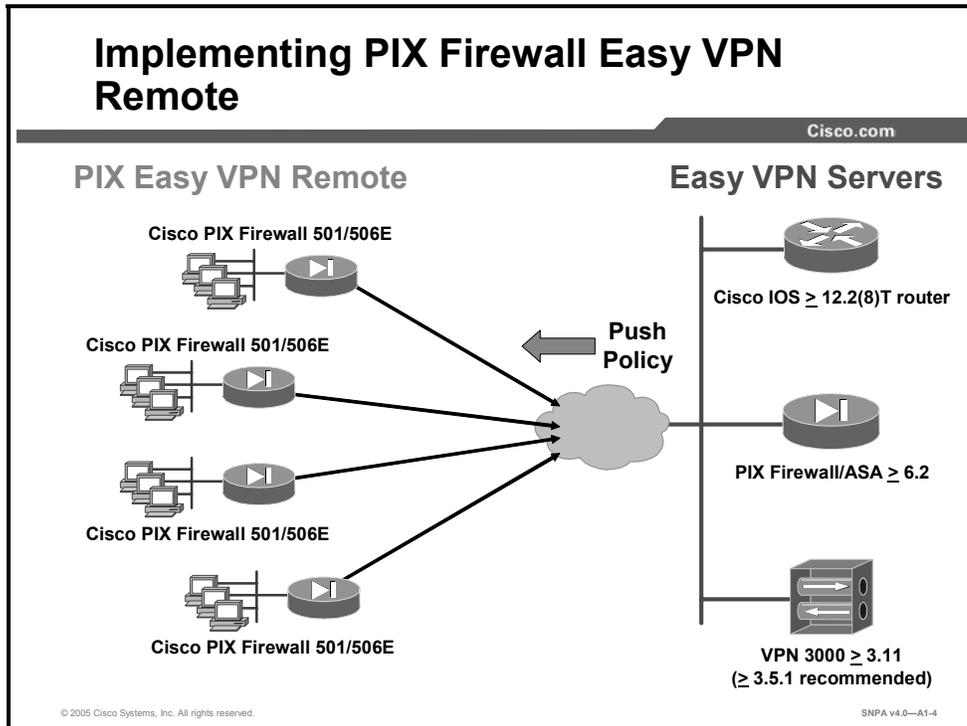
When you are using PIX Security Appliance Software v6.2 or v6.3, you can use a PIX Security Appliance 501 or PIX Security Appliance 506/506E as an Easy VPN Remote device when connecting to an Easy VPN Server, such as a Cisco VPN 3000 Concentrator, Cisco IOS router, or another security appliance. The Easy VPN Remote device, sometimes called a "hardware client," allows the PIX Security Appliance to establish a VPN tunnel to the Easy VPN Server. Hosts running on the LAN behind the PIX Security Appliance can connect through the Easy VPN Server without individually running any VPN client software.

Each Easy VPN Remote device is assigned to a group. As Easy VPN Remote devices establish a VPN tunnel to the Easy VPN Server, the attributes associated with their group are pushed to the Easy VPN Remote device.

Easy VPN Remote Configuration

This topic describes basic commands that are useful for configuring the PIX Security Appliance.

Easy VPN Remote Client Configuration

```
pixfirewall(config)#

vpnclient group_name password preshared_key
```
• **Indicates group name and preshared key**

```
vpnclient username { xauth_username} password { xauth_password}
```
• **Indicates VPN client extended authentication username and password**

```
vpnclient server { ip_primary} [ ip_secondary_n]
```
• **Indicates easy VPN Server IP address**

```
pix1(config)# vpngroup training password  cisco123
pix1(config)# vpnclient username student1 password training
pix1(config)# vpnclient server 192.168.1.2
```

SNPA v4.0—A1-6

The Easy VPN Server controls the policy enforced on the PIX Security Appliance Easy VPN Remote device. However, to establish the initial connection to the Easy VPN Server, you must complete some configuration locally. You can perform this configuration by using Cisco PIX Device Manager (PDM) or by using the command-line interface as follows:

■ If the Easy VPN Server uses preshared keys, enter the following command:

```
vpnclient vpngroup { groupname} password { preshared_key}
```

Replace *groupname* with an alphanumeric identifier for the VPN group. Replace *preshared_key* with the encryption key to use for securing communications to the Easy VPN Server.

■ If the Easy VPN Server uses extended authentication (Xauth) to authenticate the PIX Security Appliance client, enter the following command:

```
vpnclient username { xauth_username} password {
xauth_password}
```

Replace *xauth_username* with the username assigned for Xauth. Replace *xauth_password* with the password assigned for Xauth.

■ Identify the remote Easy VPN Server by entering the following command:

```
vpnclient server { ip_primary} [ ip_secondary_n]
```

Replace *ip_primary* with the IP address of the primary Easy VPN Server. Replace *ip_secondary_n* with the IP address of one or more Easy VPN Servers. A maximum of 11 Easy VPN Servers are supported (one primary and up to ten secondary).
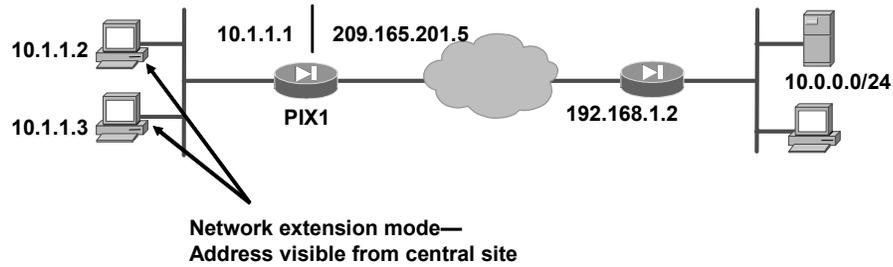
Easy VPN Client Device Mode
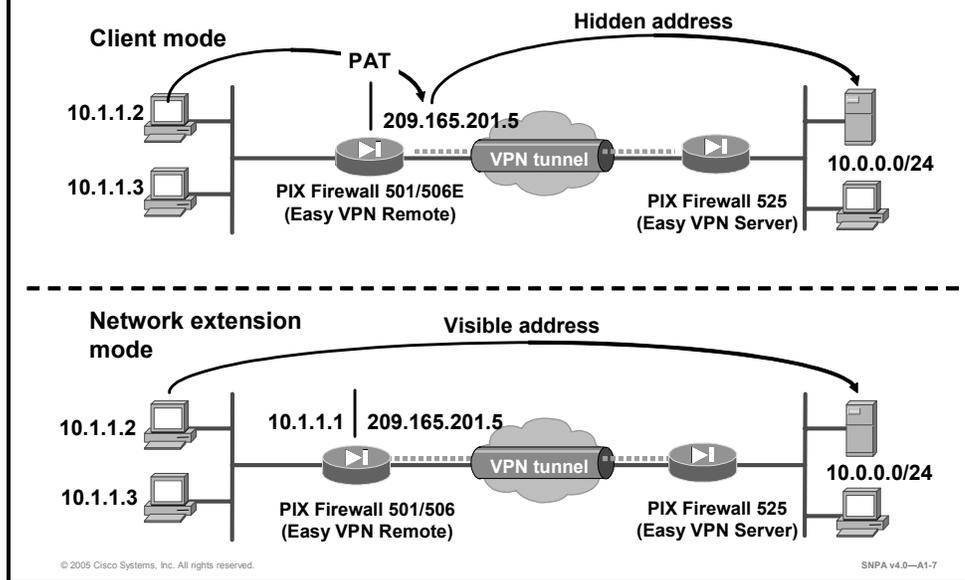
Set the Easy VPN Remote device to one of two modes, client mode or network extension mode. In client mode, the remote PIX Security Appliance applies port address translation (PAT) to all client IP addresses connected to the inside interface. In the example in the figure, when PC 10.1.1.2 attempts to connect to the server at the central site, the remote PIX Security Appliance translates the original IP address and port number using the IP address and port number of the outside interface, port address translation. Due to the translation, the IP address is not visible from the central site.

The other option is network extension mode (NEM). With NEM, the IP addresses of the inside PCs are received without change at the central site. In this instance, the IP address is visible from the central site. In the example in the figure, the remote inside PC makes a connection to a server on the central site. The original IP address, 10.1.1.2, is not translated by the remote PIX Security Appliance.

Easy VPN Client Device Mode Configuration

Cisco.com

10.1.1.2

10.1.1.1 | 209.165.201.5

PIX1

192.168.1.2

10.0.0.0/24

10.1.1.3

**Network extension mode—
Address visible from central site**

pixfirewall(config)#

```
vpnclient mode {client-mode | network-extension-mode}
```

• **Sets the easy VPN remote device mode — client of network extension mode.**

```
pix1(config)# vpnclient mode network-extension-mode
```

SNPA v4.0—A1-8

Set the Easy VPN Remote device mode by entering the following command:

```
vpnclient mode {client-mode | network-extension-mode}
```

Client mode applies Network Address Translation (NAT) to all IP addresses of clients connected to the inside (higher security) interface of the PIX Security Appliance.

Network extension mode does not apply NAT to any IP addresses of clients on the inside (higher security) interface of the PIX Security Appliance.

Enable Easy VPN Remote Device

10.1.1.2

10.1.1.3

PIX1

VPN tunnel

10.0.0.0/24
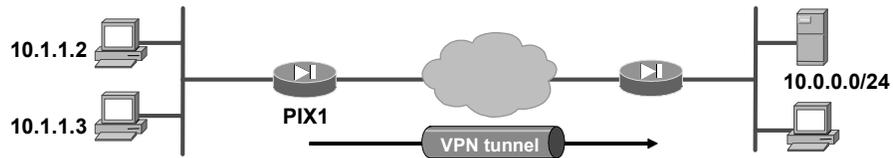
pixfirewall(config)#

```
vpnclient enable
```

• **Enables the Easy VPN Remote device**

```
pix1(config)# vpnclient enable
```
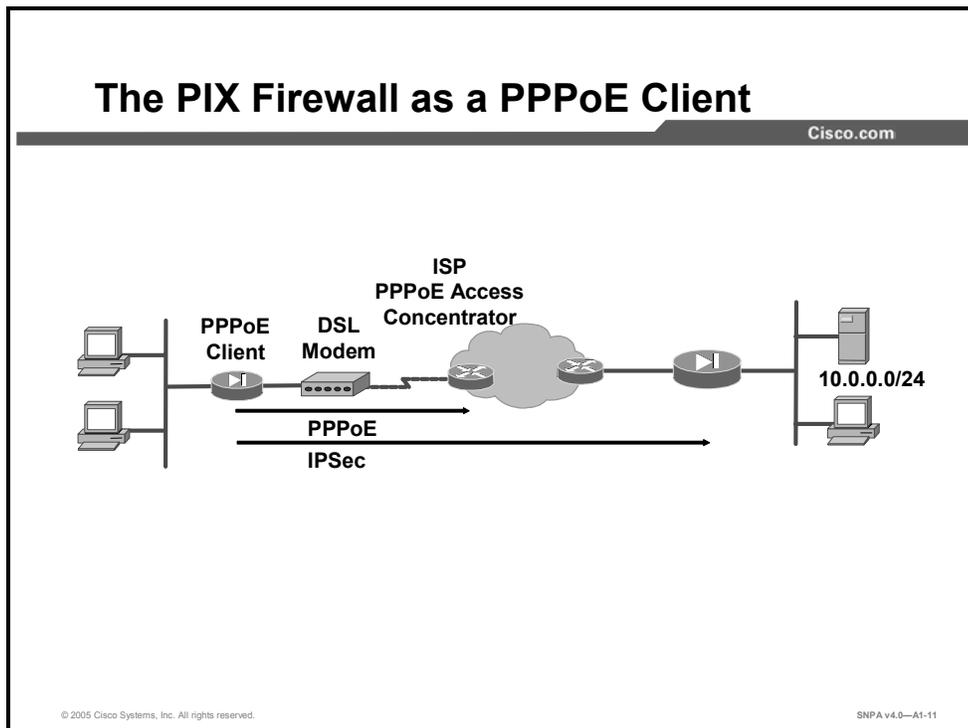
SNPA v4.0—A1-9

Enable the Easy VPN Remote device by entering the following command:

```
vpnclient enable
```

PPPoE and the PIX Security Appliance

This topic describes how the PIX Security Appliance works with Point-to-Point Protocol over Ethernet (PPPoE).

The PIX Security Appliance can be configured as a Point to Point Protocol over Ethernet (PPPoE) client. This makes it compatible with broadband offerings that require PPPoE usage. Many ISPs deploy PPPoE because it supports high-speed broadband access using their existing remote access infrastructure and because it is easy for customers to use.

Broadband connections such as DSL, cable modem, and fixed wireless deliver high-speed, always-on connections at a low cost. The PIX Security Appliance enables you to secure these broadband Internet connections.

PPPoE combines two widely accepted standards, Ethernet and Point-to-Point Protocol (PPP), to provide an authenticated method of assigning IP addresses to client systems. PPPoE is composed of these two phases:

■ Active discovery phase**:** In this phase, the PPPoE client locates a PPPoE server, called an access concentrator. A session identification is assigned and the PPPoE layer is established.

■ PPP session phase: In this phase, PPP options are negotiated and authentication is performed. After the link setup is completed, PPPoE functions as a Layer 2 encapsulation method, allowing data to be transferred over the PPP link within PPPoE headers.

After it is configured, the PPPoE client of the PIX Security Appliance automatically connects to an access concentrator of a service provider without user intervention. The maximum transmission unit (MTU) size is automatically set to 1492 bytes, the correct value to allow PPPoE to be transmitted in an Ethernet frame. All traffic flowing to, from, and through the interface is then encapsulated with PPPoE or PPP headers. The PIX Security Appliance also detects session termination and automatically attempts to reconnect.

The PIX Security Appliance PPPoE client can operate in environments where other PIX Security Appliance features are being used. For example, the following features function as usual:

- NAT on traffic to or from the outside interface or over a VPN

- URL and content filtering before transmission to or from the outside interface

- Application of Security Appliance rules on traffic before transmission to or from the outside interface or over a VPN

If the PPPoE server of your ISP distributes configuration parameters such as Domain Name System (DNS) and Windows Internet Name Service (WINS) addresses along with the IP addresses it assigns to its clients, the PIX Security Appliance PPPoE client can retrieve these parameters and automatically pass them along to its DHCP clients. The PIX Security Appliance must be configured with the *dhcpd auto_config* option for this to work. Although the PIX Security Appliance DHCP server feature functions normally with the PPPoE client enabled, its DHCP and PPPoE client features are mutually exclusive. When you configure the DHCP client on the outside interface, the PPPoE client is automatically disabled. The converse of this configuration statement is also true; when the PPPoE client is configured, the DHCP client is automatically disabled.

With PPPoE support, the PIX Security Appliance is able to provide telecommuters, branch offices, and small businesses with Security Appliance, VPN, and intrusion protection.
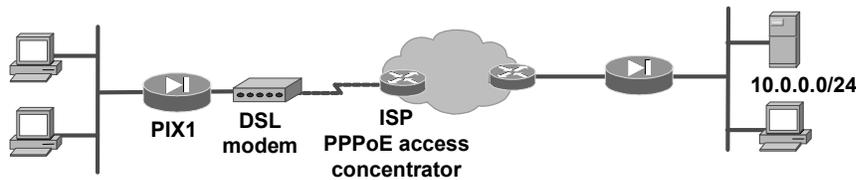
| **Note** | The PIX Security Appliance PPPoE client is not interoperable with failover, Layer 2 Tunneling Protocol (L2TP), or Point-to-Point Tunneling Protocol (PPTP). |

Configure a Virtual Private Dial-Up Networking Group

10.0.0.0/24

PIX1   DSL modem   ISP PPPoE access concentrator

pixfirewall(config)#

```
vpdn group group_name request dialout pppoe
```
• **Defines a VPDN group to be used for PPPoE**

```
vpdn group group_name ppp authentication PAP | CHAP | MSCHAP
```
• **Selects an authentication method**

```
vpdn group group_name localname username
```
• **Associates the username assigned by your ISP with the VPDN group**

```
pix1(config)# vpdn group PPPOEGROUP request dialout pppoe
pix1(config)# vpdn group PPPOEGROUP ppp authentication pap
pix1(config)# vpdn group PPPOEGROUP localname MYUSERNAME
```

SNPA v4.0—A1-12

Five steps are needed to configure the PIX Security Appliance PPPoE client. The first four steps require the use of the **vpdn** command as follows:

Step 208 Use the **vpdn group** command to define a virtual private dial-up network (VPDN) group to be used for PPPoE.

Step 209 If your ISP requires authentication, use the **vpdn group** command to select one of the following authentication protocols:

■ **Password Authentication Protocol (PAP)**

■ **Challenge Handshake Authentication Protocol (CHAP)**

■ **Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)**

Note ISPs that use CHAP or MS-CHAP may refer to the username as the remote system name, and may refer to the password as the CHAP secret.

Step 210 Use the **vpdn group** command to associate the username assigned by your ISP to the VPDN group.

The syntaxes for the **vpdn** commands are as follows:

```
vpdn group group_name request dialout pppoe
vpdn group group_name ppp authentication PAP | CHAP | MSCHAP
vpdn group group_name localname username
clear vpdn [group | username | tunnel [all | [id tunnel_id]]]
```

group_name	Descriptive name for the group.
local name *username*	Username assigned by the ISP.
username *name*	Local username. However, when used as a **clear** command option, username removes all **vpdn username** commands from the configuration.
pass	Password assigned by the ISP.
group	Removes all **vpdn group** commands from the configuration.
tunnel	Removes one or more L2TP or PPTP tunnels from the configuration. This option is not used with PPPoE.
all	Removes all L2TP or PPTP tunnels from the configuration. This option is not used with PPPoE.
id	PPPoE session identifier.
session_id	Unique session identifier.

Create VPDN Username and Password

Cisco.com

10.0.0.0/24

PIX1   DSL   ISP
       modem PPPoE access
              concentrator
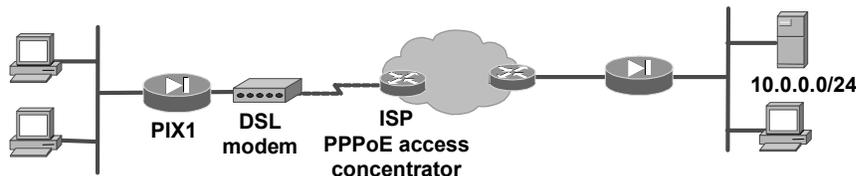
pixfirewall(config)#

```
vpdn username name password pass
```

- **Creates a username and password pair for the PPPoE connection**

```
pix1(config)# vpdn username student1 password training
```

SNPA v4.0—A1-13

Step 211   Use the **vpdn username** command to create a username and password pair for the PPPoE connection. This username and password combination is used to authenticate the PIX Security Appliance to the access concentrator. The username must be a username that is already associated with the VPDN group specified for PPPoE.

The **clear vpdn** command removes all **vpdn** commands from the configuration. The **clear vpdn group** command removes all **vpdn group** commands from the configuration, and the **clear vpdn username** command removes all **vpdn username** commands from the configuration.

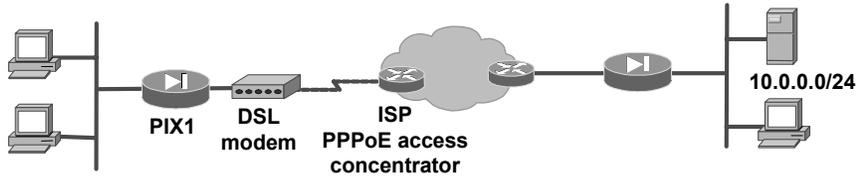The syntaxes for the **vpdn** commands are as follows:

```
vpdn username name password pass
clear vpdn [group | username | tunnel [all | [id tunnel_id]]]
```

username *name*	Local username. However, when used as a **clear** command option, username removes all **vpdn username** commands from the configuration.
pass	Password assigned by the ISP.

Enable PPPoE Client

```
pixfirewall(config)#
```

```
ip address if_name pppoe [setroute]
```

- **Enables PPPoE client**

```
pix1(config)# ip address outside pppoe
```

Step 212 PPPoE client functionality is disabled by default. Use the **ip address pppoe** command to enable PPPoE on the PIX Security Appliance.

The syntax for the **ip address pppoe** command is as follows:

```
ip address if_name pppoe [setroute]
```

if_name	The name of the outside interface of the PIX Security Appliance.
setroute	Tells the PIX Security Appliance to set the default route using the default gateway parameter that the DHCP or PPPoE server returns.

Reenter the **ip address outside pppoe** command to clear and restart a PPPoE session. This shuts down the current session and starts a new session.

The PPPoE client is only supported on the outside interface of the PIX Security Appliance. PPPoE is not supported in conjunction with DHCP, because with PPPoE the IP address is assigned by PPP. The **setroute** option causes a default route to be created if no default route exists. The default router will be the address of the access concentrator. If you use the **setroute** option when a default route is already set in the configuration, the PIX Security Appliance does not establish PPPoE. This is because it cannot overwrite an existing default gateway with one supplied by PPPoE. If you wish to use the default route from a PPPoE server, erase the default route in the configuration. The MTU size is automatically set to 1492 bytes, which is the correct value to allow PPPoE transmission within an Ethernet frame.

You can also enable PPPoE by manually entering the IP address, using the command in the following format:

```
ip address ifname ipaddress mask pppoe
```

This command causes the PIX Security Appliance to use the specified address instead of negotiating with the PPPoE server to assign an address dynamically. To use this command, replace *ifname* with the name of the outside interface of the PIX Security Appliance connected to the PPPoE server. Replace *ipaddress* and *mask* with the IP address and subnet mask assigned to your PIX Security Appliance.

The syntax for the **ip address pppoe** command is as follows:

```
ip address if_name ip_address netmask pppoe [setroute]
```

if_name	The name of the outside interface of the PIX Security Appliance.
setroute	Tells the PIX Security Appliance to set the default route using the default gateway parameter that the DHCP or PPPoE server returns.
ip_address	The IP address assigned to the PIX Security Appliance outside interface.
netmask	The subnet mask assigned to the PIX Security Appliance outside interface.

Monitoring the PPPoE Client

pixfirewall(config)#

```
show vpdn
```

- **Displays tunnel and session information**

pixfirewall(config)#

```
show vpdn session [l2tp | pptp | pppoe] [id
  session_id | packets | state | window]
```

- **Displays session information**

pixfirewall(config)#

```
show vpdn tunnel [l2tp | pptp | pppoe] [id
  tunnel_id | packets | state | summary | transport]
```

- **Displays tunnel information**

The **show vpdn** command displays PPPoE tunnel and session information. To view only session information, use the **show vpdn session** command. To view only tunnel information, use the **show vpdn tunnel** command.

The following example shows the kind of information provided by the **show vpdn** commands:

```
pix1# sh vpdn
Tunnel id 0, 1 active sessions
     time since change 65862 secs
     Remote Internet Address 172.31.31.1
    Local Internet Address 192.168.10.2
     6 packets sent, 6 received, 84 bytes sent, 0 received
Remote Internet Address is 10.0.0.1
    Session state is SESSION_UP
       Time since event change 65865 secs, interface outside
       PPP interface id is 1
       6 packets sent, 6 received, 84 bytes sent, 0 received
pix1# sh vpdn session
PPPoE Session Information (Total tunnels=1 sessions=1)
Remote Internet Address is 172.31.31.1
  Session state is SESSION_UP
    Time since event change 65887 secs, interface outside
    PPP interface id is 1
    6 packets sent, 6 received, 84 bytes sent, 0 received
pix1# sh vpdn tunnel
PPPoE Tunnel Information (Total tunnels=1 sessions=1)
Tunnel id 0, 1 active sessions
    time since change 65901 secs
    Remote Internet Address 172.31.31.1
    Local Internet Address 192.168.10.2
```

```
6 packets sent, 6 received, 84 bytes sent, 0 received
```

pixfirewall(config)#

```
show vpdn pppinterface [id intf_id]
```

- **Displays the interface identification value**

pixfirewall(config)#

```
show vpdn username [name]
```

- **Displays local usernames.**

pixfirewall(config)#

```
show vpdn group [groupname]
```

- **Displays configured groups**

pixfirewall(config)#

```
show ip address if_name pppoe
```

- **Displays detailed information about a PPPOE connection**

You can use the **show vpdn pppinterface** command when a PPPoE session is established to view the address of the access concentrator. When the PIX Security Appliance is unable to find an access concentrator, the address of the access concentrator is displayed as 0.0.0.0.

Use the **show vpdn username** command to view local usernames. Use **the show vpdn group** command to view your configured VPDN groups.

When a PPPoE session is established, you can use the **show ip address outside pppoe** command to view the IP address assigned by the PPPoE server.

The syntaxes for the **show vpdn** commands are as follows:

```
show vpdn
show vpdn session [l2tp | pptp | pppoe] [id session_id |
packets | state | window]
show vpdn tunnel [l2tp | pptp | pppoe] [id tunnel_id | packets
| state | summary | transport]
show vpdn pppinterface [id intf_id]
show vpdn username [name]
show vpdn group [groupname]
```

session_id	A unique session identifier.
tunnel_id	A unique tunnel identifier.
intf_id	A unique identifier for a PPP virtual interface. A PPP virtual interface is created for each PPTP or PPPoE tunnel.
name	The local username.
group_name	The VPDN group name. The VPDN group_name is an ASCII string to denote a VPDN group. The maximum length is 63 characters.

The syntax for the **show ip address pppoe** command is as follows:

```
show ip address if_name pppoe
```

if_name	The internal or external interface name designated by the **nameif** command.

Debugging the PPPoE Client

pixfirewall(config)#

```
debug pppoe event | error | packet
```

• **Enables debugging for the PPPoE client**

Use the **debug pppoe** command to enable debugging for the PPPoE client.

The syntax for the **debug pppoe** command is as follows:

```
debug pppoe event | error | packet
```

event	Displays protocol event information.
error	Displays error messages.
packet	Displays packet information.

DHCP Server Configuration

This topic describes how to configure the PIX Security Appliance DHCP server on the PIX Security Appliance 501 or PIX Security Appliance 506/506E.

DHCP

Cisco.com

The PIX Firewall DHCP server can be used to dynamically assign:

- **An IP address and subnet mask**
- **The IP address of a DNS server**
- **The IP address of a WINS server**
- **A domain name**
- **The IP address of a TFTP server**
- **A lease length**

SNPA v4.0—A1-19

DHCP provides automatic allocation of reusable network addresses on a TCP/IP network. This provides ease of administration and dramatically reduces the margin of human error. Without DHCP, IP addresses must be manually entered at each computer or device that requires an IP address.

DHCP can also distribute other configuration parameters, such as DNS and WINS server addresses and domain names. The host that distributes the addresses and configuration parameters to DHCP clients is called a DHCP server. A DHCP client is any host using DHCP to obtain configuration parameters.

Because DHCP traffic consists of broadcasts and a significant goal of router configuration is to control unnecessary proliferation of broadcast packets, it may be necessary to enable forwarding of DHCP broadcast packets on routers that lie between your DHCP server and its clients. Use the **ip helper-address** interface configuration command to have the Cisco IOS software forward these broadcasts. The address specified in the command should be that of the DHCP server.

Note   WINS registers Network Basic Input/Output System (NetBIOS) computer names and resolves them to IP addresses.


Any PIX Security Appliance that runs software v5.2 or higher supports a DHCP server and client. In a network environment secured by a PIX Security Appliance, PC clients connect to the PIX Security Appliance and establish network connections to access an enterprise or corporate network. As a DHCP server, the PIX Security Appliance provides these PCs (its DHCP clients) with the networking parameters necessary for accessing the enterprise or corporate network, and once inside the network, the PIX Security Appliance provides the network services to use, such as the DNS server. As a DHCP client, the PIX Security Appliance is able to obtain an IP address, subnet mask, and, optionally, a default route from a DHCP server.

Currently, the PIX Security Appliance can distribute configuration parameters only to clients that are physically connected to the subnet of its inside interface.

DHCP Server

1. **DHCPDISCOVER: The client seeks an address.**
2. **DHCPOFFER: The server offers 10.1.1.2.**
3. **DHCPREQUEST: The client requests 10.1.1.2.**
4. **DHCPACK: The server acknowledges the assignment of 10.1.1.2.**

Internet

DHCP pool
10.1.1.2–10.1.1.20
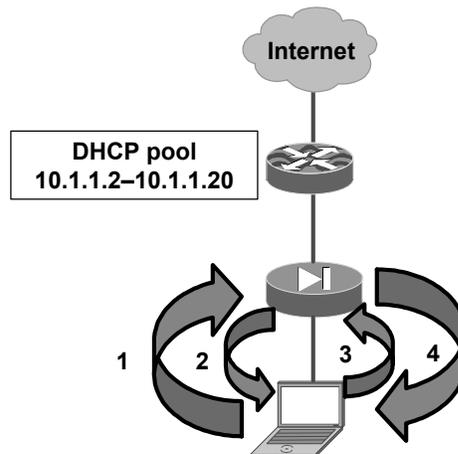
SNPA v4.0—A1-20

DHCP communication consists of several broadcast messages passed between the DHCP client and DHCP server. The following events occur during this exchange:

26. The client broadcasts a DHCPDISCOVER message on its local physical subnet to locate available DHCP servers.

27. Any reachable DHCP server may respond with a DHCPOFFER message that includes an available network address and other configuration parameters.

28. Based on the configuration parameters offered in the DHCPOFFER messages, the client chooses one server from which to request configuration parameters. The client broadcasts a DHCPREQUEST message requesting the offered parameters from one server and implicitly declining offers from all others.

29. The server selected in the DHCPREQUEST message responds with a DHCPACK message containing the configuration parameters for the requesting client. If the selected server has since become unable to satisfy the DHCPREQUEST (for example, in case the requested network address has already been allocated), the server responds with a DHCPNAK message. The client receives either the DHCPNAK or the DHCPACK containing the configuration parameters.

Note	The PIX Security Appliance DHCP server does not support BOOTP requests and failover configurations.

Configuring the PIX Firewall as a DHCP Server

- **Step 1: Assign a static IP address to the inside interface.**
- **Step 2: Specify a range of addresses for the DHCP server to distribute.**
- **Step 3: (Optional.) Specify the IP address of the DNS server.**
- **Step 4: (Optional.) Specify the IP address of the WINS server.**
- **Step 5: (Optional.) Configure the domain name.**
- **Step 6: (Optional.) Specify the IP address of the TFTP server.**
- **Step 7: Specify the lease length (default = 3600 seconds).**
- **Step 8: Enable DHCP.**

SNPA v4.0—A1-21

Complete the following steps to enable DHCP server support on the PIX Security Appliance:

Step 213   Assign a static IP address to the inside interface by using the **ip address** command.

Step 214   Specify a range of addresses for the DHCP server to distribute by using the **dhcpd address** command.

Step 215   Specify the IP address of the DNS server that the client will use by using the **dhcpd dns** command. This step is optional.

Step 216   Specify the IP address of the WINS server the client will use by using the **dhcpd wins** command. This step is also optional.

Step 217   Configure the domain name the client will use by using the **dhcpd domain** command. This step is optional.

Step 218   Specify the IP address of the TFTP server. This step is also optional.

Step 219   Specify the lease length to grant the client by using the **dhcpd lease** command.

Step 220   Enable the DHCP daemon within the PIX Security Appliance to listen for DHCP client requests on the enabled interface by using the **dhcpd enable** command.

Configure DHCP Address Pool

Cisco.com

10.1.1.2

DHCP server

ACS

10.0.0.0/24

10.1.1.3

DHCP address pool:
10.1.1.2-10.1.1.15
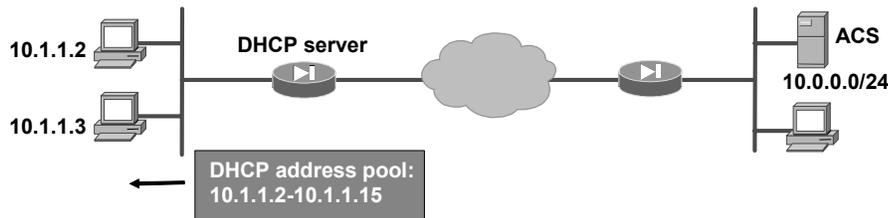
pixfirewall(config)#

```
dhcpd address ip1[-ip2][if_name]
```

• **Specifies a range of addresses for DHCP to assign**

```
pix1(config)# dhcpd address 10.1.1.2-10.1.1.15 inside
```

SNPA v4.0—A1-22

The **dhcpd address** command specifies the range of IP addresses for the server to distribute. The address pool of a PIX Security Appliance DHCP server must be within the same subnet as the PIX Security Appliance interface that is enabled. In other words, the client must be physically connected to the subnet of a PIX Security Appliance interface. Up to 256 addresses can be included in the pool. The default for the PIX Security Appliance interface name is the inside interface, which is the only interface currently supported. The **no dhcpd address** command removes the DHCP server address pool.
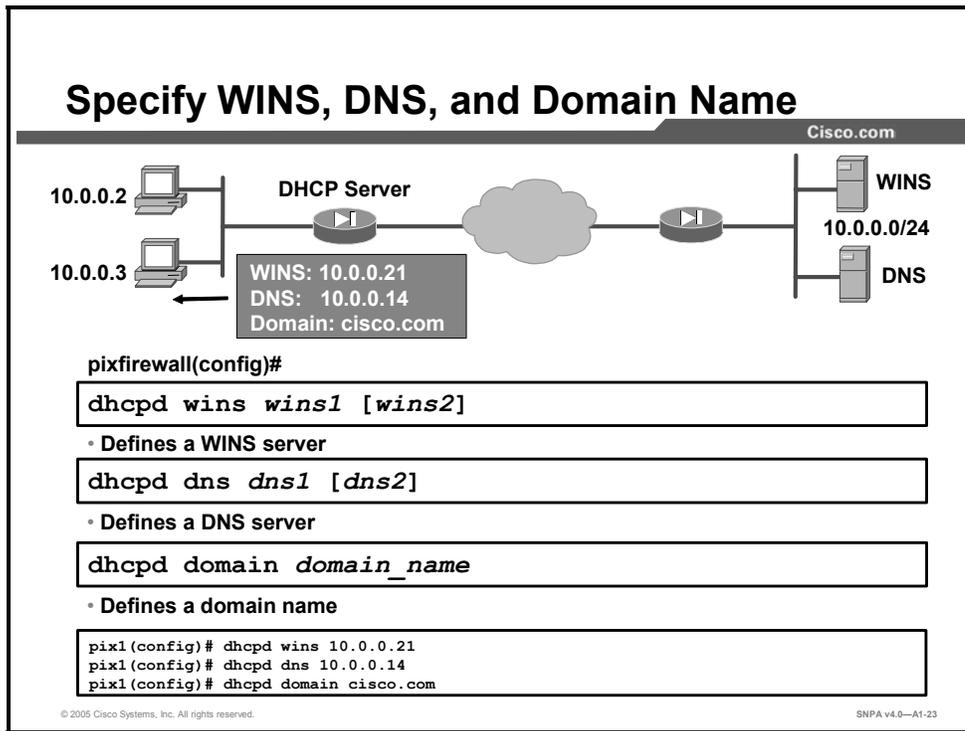
The syntax for the **dhcpd address** command is as follows:

```
dhcpd address ip1 [-ip2] [if_name]
```

address *ip1 [ip2]*	The IP pool address range. The size of the pool is limited to 256 addresses.
if_name	Name of the PIX Security Appliance interface. The default is the inside interface. The PIX Security Appliance DHCP server daemon can only be enabled on the inside interface.

Note	The DHCP address pool is limited to 32 addresses for a PIX Security Appliance 501 with a 10-user license. With the 50-user license, 128 addresses are supported.

Specify WINS, DNS, and Domain Name

Cisco.com

```
pixfirewall(config)#
```

```
dhcpd wins wins1 [wins2]
```

• Defines a WINS server

```
dhcpd dns dns1 [dns2]
```

• Defines a DNS server

```
dhcpd domain domain_name
```

• Defines a domain name

```
pix1(config)# dhcpd wins 10.0.0.21
pix1(config)# dhcpd dns 10.0.0.14
pix1(config)# dhcpd domain cisco.com
```

SNPA v4.0—A1-23

The **dhcpd dns** command specifies the IP address of the DNS server for DHCP clients. Up to two DNS servers can be specified with this command. Use the **no dhcpd dns** command to remove the DNS IP addresses from your configuration.

The syntax for the **dhcpd dns** command is as follows:

```
dhcpd dns dns1 [dns2]
```

dns *dns1 [dns2]*	The IP addresses of the DNS servers for the DHCP client. The second server address is optional.

Specify the IP addresses or addresses of the WINS server or servers the client will use. You can specify up to two WINS servers.

The syntax for the **dhcpd dns** command is as follows:

```
dhcpd wins wins1 [wins2]
```

wins *wins1 [wins2]*	The IP addresses of the Microsoft NetBIOS name servers (WINS server). The second server address is optional.

Specify the domain name the client will use.

The syntax for the **dhcpd domain** *domain_name* command is as follows:

```
dhcpd domain domain_name
```

domain *domain_name*	The DNS domain name. For example, example.com.

DHCP Option 66 and 150

10.1.1.2

DHCP server

10.0.0.0/24

TFTP server
10.0.0.11

Option 150: 10.0.0.11
Option 66: 10.0.0.11

```
pixfirewall(config)#
```
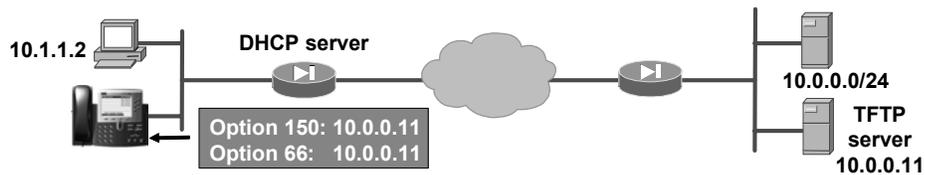
```
dhcpd option 66 ascii {server_name | server_ip_str}
```

 • **Distributes TFTP server for IP Phone connections**

```
dhcpd option 150 ip server_ip1 [server_ip2]
```

 • **Distributes list of TFTP servers for IP Phone connections**

```
pix1(config)# dhcpd option 150 ip 10.0.0.11
pix1(config)# dhcpd option 66 ip 10.0.0.11
```

SNPA v4.0—A1-24

The **dhcpd option** commands enable the PIX Security Appliance DHCP server to distribute the IP address of a TFTP server to serve DHCP clients. These options are useful for IP Phones, which may need to obtain configuration files from a TFTP server. With the **dhcpd option 66** command, the PIX Security Appliance distributes the IP address of a single TFTP server. With the **dhcpd option 150** command, it distributes a list of TFTP servers. You can remove the **dhcpd option** commands by using their **no** forms.

The syntax for the **dhcpd option** commands is as follows:

```
dhcpd option 66 ascii {server_name | server_ip_str}
dhcpd option 150 ip server_ip1 [ server_ip2]
```

server_ip(1,2)	Specifies the IP addresses of a TFTP server.
server_ip_str	Any combination of characters used to identify the server. For example, this could have the form of an IP address, such as 1.1.1.1, but is treated as a character string.
server_name	Specifies an ASCII character string representing the TFTP server.

Setting DHCP Lease Length

DHCP server

10.1.1.2

10.1.1.3

ACS

10.0.0.0/24
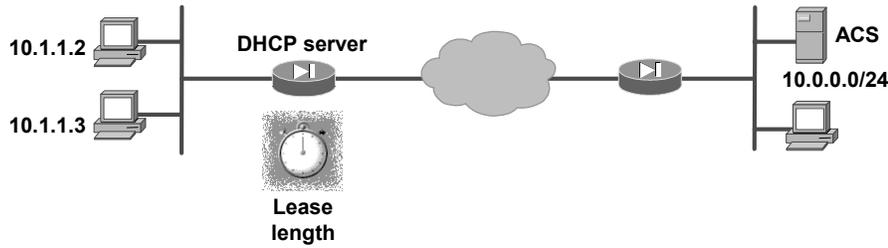
Lease
length

pixfirewall(config)#

```
dhcpd lease lease_length
```

- **Specifies DHCP lease length**

```
pix1(config)# dhcpd lease 3000
```

SNPA v4.0—A1-25

The **dhcpd lease** command specifies the amount of time in seconds that the client can use the assigned IP address. The default is 3600 seconds. The minimum lease length is 300 seconds, and the maximum lease length is 2,147,483,647 seconds.

The syntax for the **dhcpd lease** command is as follows:

```
dhcpd lease lease_length
```

lease *lease_length*	The length of the lease in seconds granted to the DHCP client from the DHCP server. The lease indicates how long the client can use the assigned IP address. The default is 3600 seconds. The minimum lease length is 300 seconds, and the maximum is 2,147,483,647 seconds.

Enable DHCP

Cisco.com

```
10.1.1.2          DHCP server                              ACS
                                                           10.0.0.0/24
10.1.1.3
```
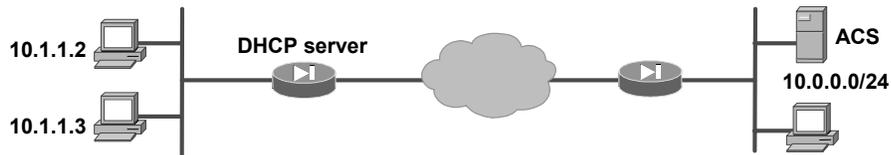
pixfirewall(config)#

```
dhcpd enable [if_name]
```

• **Enables DHCP server**

```
pix1(config)# dhcpd enable inside
```

SNPA v4.0—A1-26

Enable the DHCP daemon within the PIX Security Appliance to listen for DHCP client requests on the enabled interface by executing the **dhcpd enable** command. Currently, you can only enable the DHCP server feature on the inside interface, which is the default. Use the **no** form of the command to disable the DHCP daemon.

The syntax for the **dhcpd enable** command is as follows:

```
dhcpd enable [if_name]
```

if_name	Name of the PIX Security Appliance interface. The default is the inside interface. The DHCP server daemon can only be enabled on the inside interface.

DHCP Server Auto Configuration

WINS: 10.0.0.21
DNS: 10.0.0.15
Domain: cisco.com

IP Address: 10.1.1.2

WINS: 10.0.0.21
DNS: 10.0.0.15
Domain: cisco.com

DHCP server

DHCP client

pixfirewall(config)#
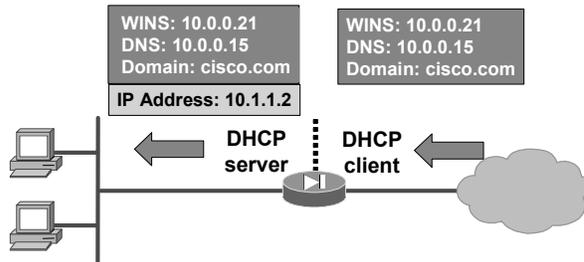
```
dhcpd auto_config[client_ifx_name]
```

- **Enables the PIX Firewall to automatically configure DNS, WINS, and domain name values from the DHCP client to the DHCP server**

```
pix1(config)# ip address outside dhcp
pix1(config)# dhcpd address 10.1.1.2-10.1.1.20 inside
pix1(config)# dhcpd auto_config
pix1(config)# dhcpd enable inside
```

SNPA v4.0—A1-27

The PIX Security Appliance can be a DHCP server, a DHCP client, or a DHCP server and client simultaneously. DHCP server and client support enables you to automatically leverage the DNS, WINS, and domain name values obtained by the PIX Security Appliance DHCP client for use by the hosts served by the PIX Security Appliance DHCP server.

Use the **dhcpd auto_config** command to enable the PIX Security Appliance to automatically pass configuration parameters it receives from a DHCP server to its own DHCP clients. DHCP must be enabled with the **dhcpd enable** command in order to use the **dhcpd auto_config** command. Use the **no dhcpd auto_config** command to disable the auto_config feature.

The syntax for the **dhcp auto_config** command is as follows:

```
dhcpd auto_config [client_ifx_name]
no dhcpd auto_config [client_ifx_name]
```

auto_config	Enables the PIX Security Appliance to automatically configure DNS, WINS, and domain name values from the DHCP client to the DHCP server.
client_ifx_name	Supports only the outside interface at this time. When more interfaces are supported, this argument will specify which interface supports the DHCP auto_config feature.

debug dhcpd and *clear dhcpd* Commands

pixfirewall(config)#

```
debug dhcpd event | packet
```

- **Displays information associated with the DHCP server**

pixfirewall(config)#

```
clear dhcpd
```

- **Removes all** dhcpd **command statements from the configuration**

The **debug dhcpd** command displays information associated with the DHCP server. Use the **debug dhcpd event** command to display event information about the DHCP server, and use the **debug dhcpd packet** command to display packet information about the DHCP server. Use the **no** form of the **debug dhcpd** command to disable debugging.

The syntax for the **debug dhcpd** command is as follows:

```
debug dhcpd event | packet
```

dhcpd event	Displays event information associated with the DHCP server.
dhcpd packet	Displays packet information associated with the DHCP server.

The **clear dhcpd** command can be used to clear all **dhcpd** commands, and binding and statistics information. Use the **clear dhcpd** command with no options to remove all **dhcpd** command statements from the configuration.

The syntax for the **clear dhcpd** command is as follows:

```
clear dhcpd [binding | statistics]
```

bindings	The binding information for a given server IP address and its associated client hardware address and lease length.
statistics	Statistical information, such as address pool, number of bindings, malformed messages, sent messages, and received messages.

Summary

This topic summarizes what you learned in this lesson.

Summary

- **Easy VPN Remote can operate in client or network extension mode.**
- **The PIX Firewall can function as a DHCP client and DHCP server.**
- **Configuring the PIX Firewall as a PPPoE client enables it to secure broadband Internet connections such as DSL.**

SNPA v4.0—A1-29

Appendix 2

Firewall Services Module

Overview

The Cisco Firewall Services Module (FWSM) is based on Cisco PIX Security Appliance technology, and therefore offers the same security and reliability. Many of the configuration commands are similar, if not identical, between the FWSM and the security appliances. This appendix describes the similarities and differences between a FWSM and a security appliance. The focus of this appendix is on initializing the FWSM module in a Cisco Catalyst switch.

Objectives

Upon completing this appendix, you will be able to initialize a Firewall Services Module. This ability includes being able to meet these objectives:

- Describe the FWSM features and benefits
- Explain the similarities and differences between the FWSM and the PIX Security Appliance
- Describe a typical deployment scenario for the FWSM
- Configure the switch VLANs
- Assign VLAN-group to a FWSM
- Configure the FWSM interfaces
- Prepare the FWSM to work with PDM

FWSM Overview

This topic describes the Cisco FWSM.

FWSM Key Features

Key features of FWSM, based on Version 2.2, include the following:

- **Brings switching and firewalls into a single chassis**
- **Based on PIX Firewall technology**
- **Supports transparent or routed firewall mode**
- **Up to 100 security contexts**
  - **Up to 256 VLANs per context**
  - **Up to 1000 VLANs all contexts**
- **5-Gbps throughput**
- **One million concurrent connections**
- **100,000 connections per second**
- **Multiple blades supported in one chassis (4 maximum)**
- **Dynamic routing via RIP v1 and v2 and OSPF**
- **High availability via intra- or inter-chassis stateful failover**

SNPA v4.0—A2-3

The Cisco FWSM is an integrated module for the Cisco Catalyst 6500 Series Switch and the Cisco 7600 Series Internet Router. The Cisco Catalyst 6500 provides intelligent services such as firewall capability, intrusion detection, and virtual private networking, along with multilayer LAN, WAN, and metropolitan-area network (MAN) switching capabilities. The Cisco 7600 Series Internet Router offers optical WAN and MAN networking with line-rate IP services at the network edge.

The Cisco FWSM is a high-performance firewall solution, providing 5 Gbps of throughput per module and scaling to 20 GB of bandwidth with multiple modules in one chassis. The FWSM is completely VLAN-aware, offers dynamic routing, and is fully integrated within the Cisco Catalyst 6500 Series switches. The FWSM is based on Cisco PIX Security Appliance technology, and therefore offers the same security and reliability as the Cisco ASA and PIX security appliances. The FWSM can run in one of the following modes:

■ **Routed:** The FWSM is considered to be a router hop in the network. It performs Network Address Translation (NAT) between connected networks, and can use Open Shortest Path First (OSPF) or passive Routing Information Protocol (RIP) in single-context mode.

■ **Transparent:** The FWSM is not a router hop. The FWSM connects the same network on its inside and outside ports, but each port must be on a different VLAN.

FWSM and PIX Firewall Feature Comparison

	FWSM	Security Appliance
Performance	5 Gbps	1.7 Gbps
VLANs	1000	150
Interfaces	Internal VLANS	External Interfaces
IDS SIgnatures	No	Yes
VPN Functionality	No	Yes
Traffic	Explicitly denied	Allowed higher to lower security level

SNPA v4.0—A2-4

Although a FWSM may be installed in the Catalyst 6500 Series switches and the Cisco 7600 Series routers, the FWSM runs its own operating system. The FWSM operating system is based on the PIX Security Appliance operating system. Although the FWSM operating system is similar to the PIX Security Appliance operating system, there are some differences, as follows:

■ The FWSM operating system performs better than the PIX Security Appliance operating system.

■ The FWSM supports more VLANs.

■ The FWSM does not include any external physical interfaces. Instead, it uses internal VLANs.

■ Termination of VPN connections for traffic flowing through the FWSM is not supported on a FWSM. The Cisco Catalyst 6500 provides intelligent services such as intrusion detection, via Cisco Intrusion Detection System Module (IDSM), and virtual private networking via VPN service modules (VPNSM).

■ By default, all traffic is explicitly denied on a FWSM.

FWSM Hardware and Software Requirements

The FWSM has the following requirements for the Catalyst 6500 switch:

- **Supervisor 1A and Multilayer Switch Feature Card 2 (MSFC2)**
- **Supervisor 2 with MSFC2**
- **Supervisor 720**
- **Cisco IOS Software Release 12.1(13)E or higher when using the Supervisor 2 option**
- **Cisco IOS Software Release 12.2(14)SX1 or higher when using the Supervisor 720**
- **CatOS minimum Software Release 7.5(1) or higher when using the Supervisor 2**
- **CatOS minimum Software Release 8.2(1) or higher when using the Supervisor 720**

SNPA v4.0—A2-5

The FWSM occupies one slot in a Cisco Catalyst 6500 switch. Up to four FWSM modules can be installed in the same switch chassis. The FWSM has the following requirements for the Catalyst 6500 switch:

- Supervisor 1A and Multilayer Switch Feature Card 2 (MSFC2)

- Supervisor 2 with MSFC2

- Supervisor 720

- Cisco IOS Software Release 12.1(13)E or higher when using the Supervisor 2 option

- Cisco IOS Software Release 12.2(14)SX1 or higher when using the Supervisor 720

- CatOS minimum Software Release 7.5(1) or higher when using the Supervisor 2

- CatOS minimum Software Release 8.2(1) or higher when using the Supervisor 720

Configuration Support

Configuration options include the following:

- **Console to command-line interface**
- **Telnet to inside interface of FWSM**
- **Telnet over IPSec to outside interface of FWSM**
- **Secure Shell Protocol (SSH) to CLI**
- **Secure Socket Layer (SSL) to PIX Device Manager**
- **CiscoWorks VMS for firewalls**

　　　　　　　　SNPA v4.0—A2-6

There are several configuration and management options for FWSM, including the following:

- Console to command-line interface

- Telnet to inside interface of FWSM

- Telnet over IPSec to outside interface of FWSM

- Secure Shell Protocol (SSH) to CLI

- Secure Socket Layer (SSL) to PIX Device Manager

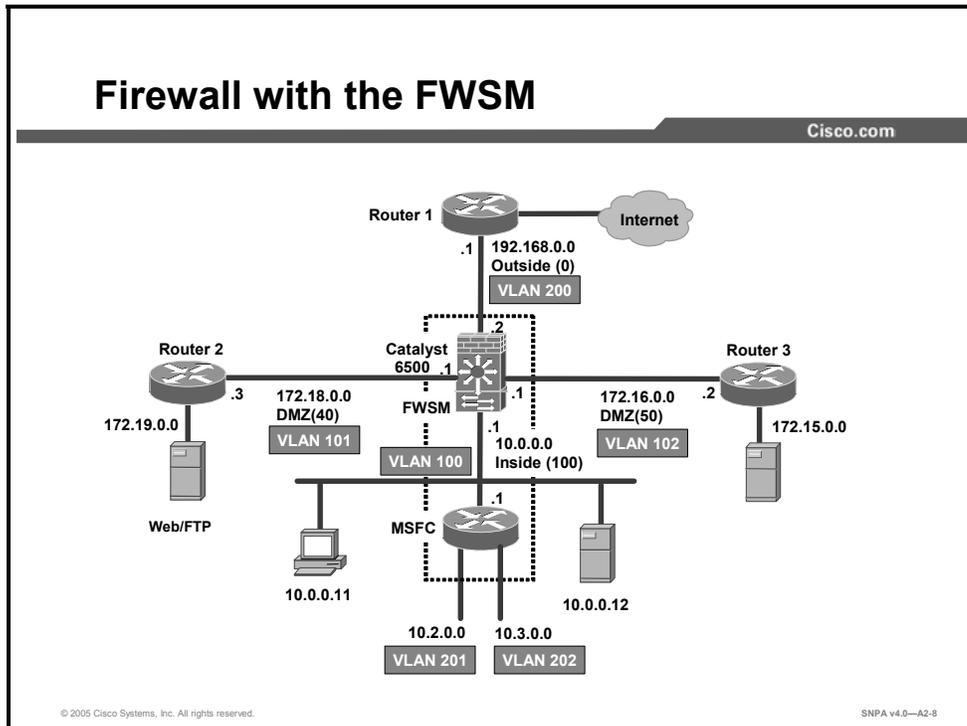- CiscoWorks Virtual Private Network/Security Management Solution (VMS) for firewalls

Note　　All FWSM interfaces, including the console, are mapped via VLANs.

Network Model

This topic describes typical FWSM deployments and traffic flow.

You can install the FWSM in the Catalyst 6500 Series switches and the Cisco 7600 Series routers. The FWSM does not include any external physical interfaces, but instead uses VLAN interfaces. You assign these VLANs to physical switch ports, and hosts connect to those ports. VLANs to be protected are associated with the FWSM VLAN group. When communication occurs between these protected VLANs, the FWSM is in the available path between the VLANs, enabling traffic to be statefully inspected.

The FWSM configuration has the following characteristics:

■ Each firewall interface is uniquely associated with a VLAN, a security level, and an IP address.

■ An interface is protected by a firewall depending on where the interface is used. The FWSM module interfaces are firewall protected, while all other interfaces in the system are considered to be outside the firewall. Each firewall interface has a fixed VLAN. In the example in the figure, traffic between VLAN 201 and 202 is not routed through the FWSM. Traffic between VLAN 101 and 201 is routed through the FWSM.

■ Traffic from all of the non-firewall VLANs in the switch (those not recognized by the FWSM module) is routed through the Multilayer Switch Feature Card (MSFC) without being stopped by the firewall. In the example in the figure, traffic between VLAN 201 and 202 is routed by the MSFC, not the FWSM.

■ The FWSM can be configured to operate in transparent mode or routed mode.

Routed Firewall and Transparent Firewall Modes

Routed Firewall Mode

- **FWSM is considered to be a router hop in the network.**

- **It performs NAT between connected networks.**

- **OSPF or passive RIP (in single context mode).**

- **Supports up to 256 interfaces per context, with a maximum of 1000 interfaces across all contexts.**

Transparent Firewall Mode

- **FWSM acts like a "bump in the wire" and is not a router hop.**

- **The FWSM connects the same network on its inside and outside ports, but each port must be on a different VLAN.**

- **No dynamic routing protocols or NAT.**

- **Transparent mode only supports two interfaces per context.**

SNPA v4.0—A2-9

A FWSM can be configured to operate in transparent or routed mode. In routed mode, the FWSM is considered to be a router hop in the network. It performs NAT between connected networks, and can use OSPF or passive RIP in single-context mode. Routed mode supports up to 256 interfaces per context, with a maximum of 1000 interfaces across all contexts.

In transparent mode, the FWSM is not a router hop. The FWSM connects the same network on its inside and outside ports, but each port must be on a different VLAN. No dynamic routing protocols or NAT are required. Transparent mode only supports two interfaces, an inside interface and an outside interface.

You might use a transparent firewall to simplify your network configuration. Transparent mode is also useful if you want the firewall to be invisible to attackers. You can also use a transparent firewall for traffic that would otherwise be blocked in routed mode. For example, a transparent firewall can allow multicast streams.

Security Contexts

- **You can partition a single FWSM into multiple virtual firewalls, known as security contexts.**
- **Each context is an independent system, with its own security policy, interfaces, and administrators.**
- **Multiple contexts are equivalent to having multiple stand-alone firewalls.**

Internet

Switch

VLAN 100

MSFC

VLAN 200

Admin Context   Context A   Context B   Context C

VLAN 201   VLAN 202   VLAN 203   VLAN 204

Admin Network   Inside Customer A   Inside Customer B   Inside Customer C
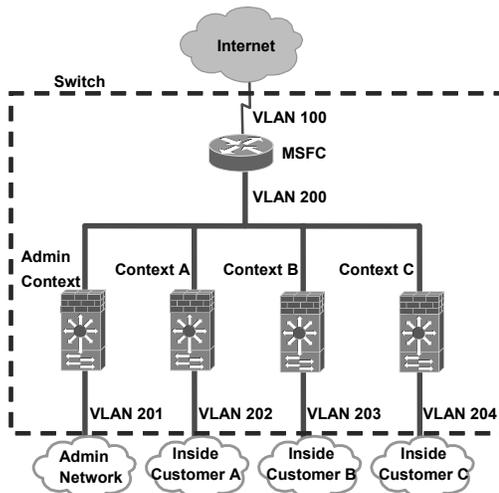
SNPA v4.0—A2-10

You can partition a single FWSM into multiple virtual firewalls, known as security contexts. Each context is an independent system, with its own security policy, interfaces, and administrators. Multiple contexts are equivalent to having multiple stand-alone firewalls.

If desired, you can allow individual context administrators to implement the security policy on the context. The overall system administrator controls some of the resources so that one context cannot affect other contexts inadvertently, such as VLANs and system resources.

You can add and manage contexts by configuring them in the system configuration, which identifies basic settings for the card. The system administrator has privileges to manage all contexts. The system configuration does not include any network interfaces or network settings for itself; rather, when the system needs to access network resources (such as downloading the contexts from the server), it uses one of the contexts that is designated as the Admin context.

The Admin context is just like any other context, except that when a user logs into the Admin context (for example, over an SSH connection), that user has system administrator rights, and can access the system configuration and all other context configurations. Typically, the Admin context provides network access to network-wide resources, such as a syslog server or context configuration server.
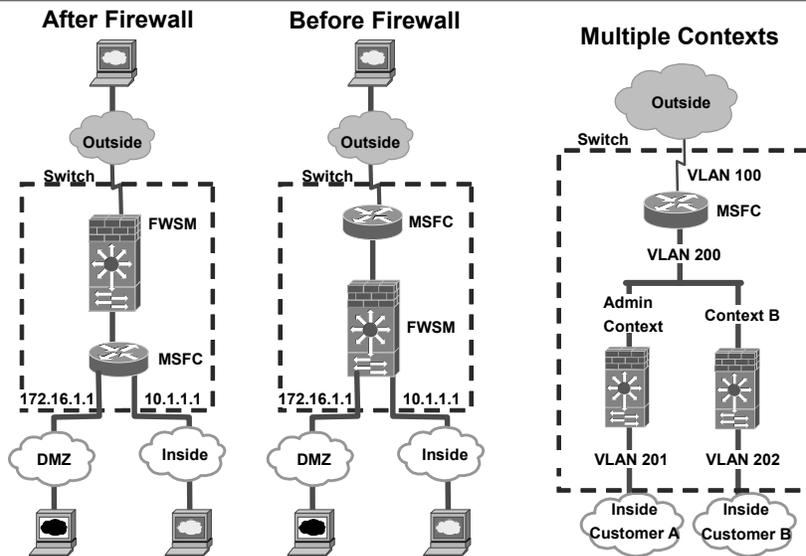
Note   In the default FWSM license, you can configure up to two contexts. For more contexts, you must purchase a context upgrade license.

MSFC placement

After Firewall

Before Firewall

Multiple Contexts

SNPA v4.0—A2-12

A Cisco Catalyst 6500 switch includes a switching supervisor and an MSFC. MSFC can be used as a router. Although you need the MSFC as part of your system, you do not have to use it in conjunction with a FWSM. If you choose to do so, you can assign one or more VLAN interfaces to the MSFC, if your switch software version supports this feature.

In single-context mode, you can place the MSFC in front of the firewall or behind the firewall. When the MSFC is located behind the firewall, traffic between the DMZ and inside VLANS is not inspected by the firewall. Only traffic to and from the outside is inspected. When the MSFC is located in front of the firewall, all traffic transits the firewall. The MSFC acts as the Internet router, terminating the traffic from the outside. The logical location of the MSFC within the switch depends on the VLANs and where the VLANs are assigned.

For multiple-context mode, if you place the MSFC behind the contexts, the MSFC will route between the contexts, which might not be your intention. The typical scenario for multiple contexts is to use the MSFC in front of all the contexts to route between the Internet and the switched networks.

Getting Started

This topic describes how to prepare to configure the FWSM.

Getting Started with the FWSM

Cisco.com

Before you can begin configuring the FWSM, complete the following tasks:

- **Verify FWSM installation.**
- **Configure the switch VLANs.**
- **Configure the FWSM VLANs.**

SNPA v4.0—A2-14

With a security appliance, you take it out of the box, hook up LAN cables, power-on the device, and then start to configure the security policy. But an FWSM is not a standalone device. It is a security module within a Catalyst chassis. Before you can begin configuring a security policy in a FWSM, you must complete the following tasks:

- Initialize the FWSM.

- Configure the switch VLANs.

- Associate VLANs with the FWSM.

You can access the switch CLI through a Telnet connection to the switch or through the switch console interface.

Verify FWSM Installation

```
Router# show module

Mod Slot Ports Module-Type              Model               Sub Status
--- ---- ----- ------------------------ ------------------- --- -
1   1    2     1000BaseX Supervisor     WS-X6K-S2U-MSFC2    yes ok
15  1    1     Multilayer Switch Feature WS-F6K-MSFC2       no  ok
2   2    48    10/100BaseTX Ethernet    WS-X6348-RJ-45      yes ok
4   4    6     Firewall Module          WS-SVC-FWM-1        no  ok
```

SNPA v4.0—A2-15

Before you can use the FWSM, you must verify that the card is installed and recognized by the switch. Enter the **show module** command to verify that the system acknowledges the new module and has brought it online.

The syntax for the **show module** command is as follows:

```
show module [mod-num | all]
```

mod-num	Number of the module and the port on the module.
all	Displays the information for all modules.

Configure the Switch VLANs

switch(config)#

```
vlan vlan_number,vlan_number,etc
```

- **Creates VLANs**

switch(config)#

```
interface vlan vlan_number
```

- **Defines a controlled VLAN on the MSFC. Assigns an IP address.**

```
switch(config)#vlan 100,200,300
switch(config-vlan)#exit
witch(config)#int vlan 100
switch(config-if)#ip address 192.168.1.2 255.255.255.0
switch(config-if)#no shut
switch(config-if)#int vlan 200
switch(config-if)#ip address 10.1.1.1 255.255.255.0
switch(config-if)#no shut
switch(config-if)#int vlan 300
switch(config-if)#ip address 172.16.1.1 255.255.255.0
switch(config-if)#no shut
```

SNPA v4.0—A2-17

You can install the FWSM in the Catalyst 6500 Series switches and the Cisco 7600 Series routers. The FWSM does not include any external physical interfaces. Instead, it uses VLAN interfaces. Hosts are connected to ports and you assign VLANs to these physical switch ports. To prevent mismatched VLANs, you should first configure a VLAN on the MSFC, and then configure the VLANs on the FWSM. VLAN IDs must be the same for the switch and the FWSM. After the MSFC VLAN is configured, you can associate specific VLANs with a FWSM.

Firewall VLAN-Group

Switch

MFC

vlan 100,200,300

FWSM
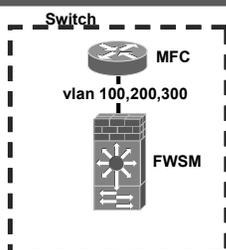
switch(config)#

```
firewall vlan-group firewall_group vlan_range
```

• **Creates a firewall group of controlled VLANs**

switch(config)#

```
firewall module module_number vlan-group firewall_group
```

• **Attaches the VLAN and firewall group to the slot where the FWSM is located**

```
switch(config)# firewall vlan-group 1 100,200,300
switch(config)# firewall module 4 vlan-group 1
```

SNPA v4.0—A2-18

The first step was to add VLANS to the MSFC. The next step is to associate VLANs to be inspected by the FWSM. You can link a VLAN with a specific FWSM by using the **firewall** command.

The **firewall vlan-group** command creates a group of firewall VLANs named by the *vlan-group* parameter. The syntax for the **firewall vlan-group** command is as follows:

```
firewall vlan-group firewall_group vlan_range
```

| *firewall_group* | Name of firewall VLAN group. |
| *vlan_range* | Numerical range of VLAN numbers to be included in the group. |

Once VLANs are assigned to a group, the **firewall module** command associates a vlan-group with a specific FWSM. Remember, a Cisco Catalyst chassis can support up to four FWSM modules.

The syntax for the **firewall module** command is as follows:
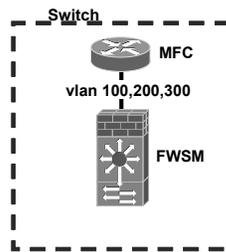
```
firewall module module_number vlan-group firewall_group
```

| *module_number* | Number of the module. |
| *firewall_group* | Name of firewall VLAN group. |

In this example, VLANs 100, 200, and 300 have been placed into Firewall VLAN-Group 1. The FWSM in Slot 4 is associated with VLAN-Group 1, VLANs 100, 200, and 300.

Verify MSFC Configuration

Switch

MFC

vlan 100,200,300

FWSM

```
switch# show firewall vlan-group
Group vlans
----- ------
1    100,200,300

switch# show firewall module
Module Vlan-groups
4      1
```

You can verify that the MSFC is properly configured for interaction with the FWSM. The **show firewall vlan-group** command verifies which VLANs are assigned to each firewall VLAN-group. The **show firewall module** command verifies that the VLAN-groups are assigned to the associated slot where the FWSM resides.

Configure the FWSM Interfaces

Cisco.com

MFC
192.168.1.2
FWSM
172.16.1.1   10.1.1.1
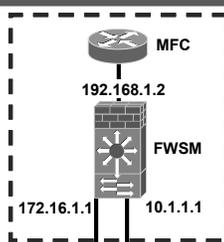
switch#

```
session slot mod {processor processor-id}
```

- **Establishes a console session with the module**
  - *Processor should always be 1*

```
switch(config)# session slot 4 processor 1
....................
fwsm(config)# hostname FWSM1
FWSM1(config)# nameif 100 outside security0
FWSM1(config)# ip address outside 192.168.1.2 255.255.255.0
FWSM1(config)# nameif 200 inside security100
FWSM1(config)# ip address inside 10.0.1.1 255.255.255.0
FWSM1(config)# nameif 300 dmz security50
FWSM1(config)# ip address dmz 172.16.1.1 255.255.255.0
```

SNPA v4.0—A2-20

The FWSM is now installed. The MSFC VLANs are configured. The FWSM VLANs are associated with a specific FSWM. The next step is to configure the security policy on the FWSM. You can access the FWSM by using the **session** command. Use the default password **cisco** for the FWSM when prompted. You will then need to enter enable mode and are prompted for an enable mode password. By default, there is no password. Simply hit **Enter**. You should change the enable password to a valid value and use this for future access to this mode.

Once on the FWSM, standard security appliance commands are used to configure interface names, add security levels, and specify IP addresses.

The example in the figure shows the use of the **nameif** command and associates VLAN 100 as the outside interface and sets the interface with a security level of 0. It also defines VLAN 200 as the inside interface. It specifies VLAN 300 as the dmz interface. In all cases, the use of the **ip address** command is used to add an IP address to each interface.

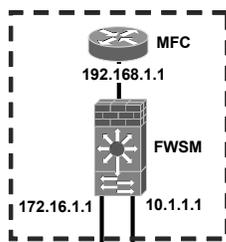The syntax of the **nameif** command is as follows:

```
nameif vlann name [security]n
```

The syntax for the **ip address** command is as follows:

```
ip address if_module ip_address [netmask]
```

Configure a Default Route

Cisco.com

```
FWSM1(config) route outside 0.0.0.0 0.0.0.0 192.168.1.1
```

- **Default route**
- **Static routes are required in multiple context mode.**

SNPA v4.0—A2-21

You may also need to add a default route. In the example in the figure, a default route is created, pointing to the VLAN 100 interface of the MSFC.

It may also be necessary to create static routes. Multiple-context mode does not support dynamic routing, so you must use static routes to reach any networks to which the FWSM is not directly connected; for example, if a router is between a network and the FWSM.

You might want to use static routes in single-context mode under the following circumstances:

- Your networks use a different router discovery protocol than RIP or OSPF.

- Your network is small and you can easily manage static routes.

- You do not want the traffic or CPU overhead associated with routing protocols.

Configure the FWSM Access-List

Cisco.com

MFC

192.168.1.2

FWSM

Inside

DMZ   Inside

10.1.1.12
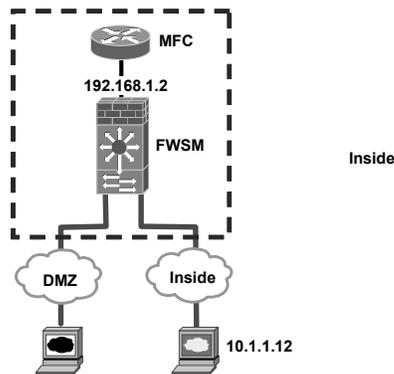
```
FWSM1(config)# access-list 200 permit ip 10.1.1.0 255.255.255.0 any
FWSM1(config)# access-group 200 in interface inside
```

- **By default all traffic is denied through the FWSM.**
- **Traffic permitted into an interface can exit through any other interface.**

SNPA v4.0—A2-22

You need to create ACLs to allow outbound as well as inbound traffic, because the FWSM, unlike security appliances, denies all inbound and outbound connections that are not explicitly permitted by ACLs. Explicit access rules need to be configured using the **access-list** command and attached to the appropriate interface using the **access-group** command to allow traffic to pass through that interface. Traffic that has been permitted into an interface can exit through any other interface. Return traffic matching the session information is permitted without an explicit ACL.

Preparing FWSM for PDM:

- **Use the *copy tftp flash* command to install the PDM image.**
- **Enable HTTP server on the FWSM.**
- **Enable specific hosts/networks to access FWSM using HTTP.**
- **Start PDM by entering the FWSM IP address in the browser.**

The FWSM 2.2 supports PDM Version 4.0.

SNPA v4.0—A2-23

Cisco PIX Device Manager (PDM) v. 4.0 is used to configure and monitor FWSM v. 2.2. The figure shows the steps needed to prepare the FWSM to use PDM. Be sure to initialize the FWSM before attempting to install PDM, as follows:

- Use the **copy tftp flash** command to copy the PDM image into FWSM flash.

      copy tftp://**10.1.1.1**/**pdm-XXX.bin flash:pdm**
      (where XXX = pdm image version number)

- Enable the HTTP server on the FWSM. Without it, PDM will not start.

      http server enable

- Identify the specific hosts and networks that can access the FWSM using HTTP.

      http 10.1.1.0 255.255.255.0 inside

  Hosts from network 10.1.1.0 (on the inside interface) are permitted http access.

- Launch the browser and enter the following address:

      https://10.1.1.0 (FWSM inside interface)

Resetting and Rebooting the FWSM

Router(config)#

```
hw-mod module module_number reset
```

• **Resets and reboots the FWSM**

```
Router(config)# hw-mod module 4 reset
Proceed with reload of module? [confirm] y
% reset issued for module 4
```

SNPA v4.0—A2-24

If you cannot reach the module through the CLI or an external Telnet session, enter the **hw-mod module module_number reset** command to reset and reboot the module. The reset process requires several minutes. The syntax for the command is as follows:

```
hw-module module module_number reset
```

module_number	Number of module you wish to reset

The example in the figure shows how to reset the module, installed in Slot 4, from the CLI.

Memory Test

Router(config)#

```
hw-module module module_number mem-test-full
```

- **Configures the FWSM to perform a full memory test when it initially boots**

```
Router(config)# hw-module module 4 mem-test-full
```

SNPA v4.0—A2-25

When the FWSM initially boots, by default it runs a partial memory test. To perform a full memory test, use the **hw-module module** *module_number* **mem-test-full** command. The syntax of the command is as follows:

```
hw-module module module_number mem-test-full
```

module_number	Number of module.

A full memory test takes more time to complete than a partial memory test, depending on the memory size. The table lists the memory and approximate boot time for a long memory test.

Memory size	Boot time
512 MB	3 minutes
1 GB	6 minutes

Summary

This topic summarizes the key points discussed in this appendix.

Summary

- **The FWSM is a line card for the Cisco Catalyst 6500 family of switches and the Cisco 7600 Series Internet routers.**
- **The FWSM is a high-performance firewall solution based on PIX Firewall Security Appliance technology.**
- **The FWSM supports transparent and routed firewall modes.**
- **The FWSM commands are almost identical to security appliance commands.**
- **PDM can be used to configure and monitor the FWSM.**

© 2005 Cisco Systems, Inc. All rights reserved.

SNPA v4.0—A2-26