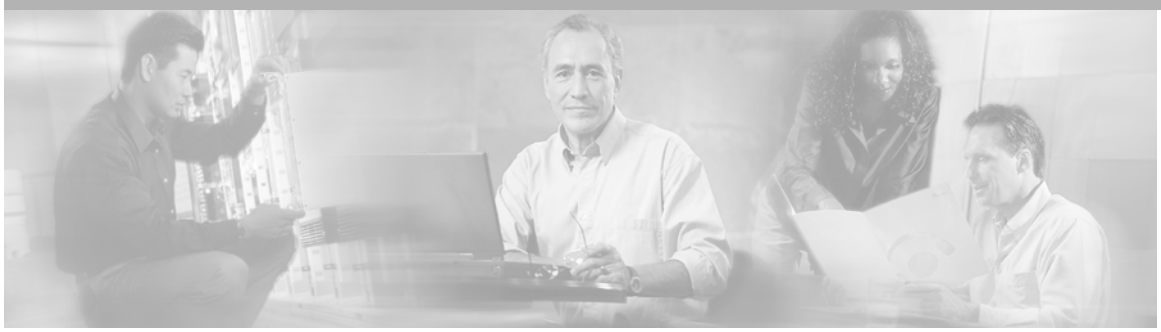
Cisco Systems



Migrating to ASA for VPN 3000 Concentrator Series Administrators

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number:
Text Part Number: OL-6940-01

CHAPTER 5

About This Guide

This guide explains how to configure many standard VPN features in the Adaptive Security Appliance (ASA) software. In most cases, instructions are given in both CLI and the device manager.

Note This guide contains instructions for fundamental VPN tasks using both CLI and ASDM. The description of each feature includes at least one example that illustrates configuration steps with a basic or simple scenario. In general, the instructions show the same values in both CLI and ASDM, although there are a few exceptions.

Audience

This guide is for system engineers (SEs) and network administrators who set up and configure ASAs for virtual private networking. These SEs and customers are familiar with virtual private networking from the perspective of a VPN 3000 Concentrator and need guidance on performing familiar tasks in the ASA software environment.

This document should help you come up to speed quickly on the new system. You should be familiar with networking equipment, basic networking concepts, virtual private networking, and the VPN 3000 Concentrator Manager.

Organization

This guide is organized as follows:

Chapter	Title	Description
Chapter 1	Feature Differences	Maps the features in the VPN 3000 Concentrator Features to those in the ASA.
Chapter 2	Introducing the ASA System	Highlights major features of the ASA that are different from the VPN 3000 Concentrator.
Chapter 3	Getting Started	Introduces the Startup wizard and the VPN wizard in the ASDM and lists the information you should have before using the wizards. Compares the Getting Started program in the VPN 3000 Concentrator with these wizards.

Chapter	Title	Description
Chapter 4	Building Basic VPN Tunnels	Shows how to configure VPN LAN-to-LAN and remote-access tunnels using CLI commands and using Adaptive Security Device Manager (ASDM). Also shows how to enroll for digital certificates.
Chapter 5	Performing Selected User Management Tasks	Shows how to configure split tunneling, client firewalls, and how to authenticate using RADIUS.
Chapter 6	Configuring Traffic Management	Shows how to configure load balancing and quality of service features.
Appendix A	Mapping Topics from VPN 3000 Series Concentrators to ASDM	Maps configuration and management topics of the VPN 3000 Concentrator Manager and ASDM.
Appendix B	Mapping Debug/Event Levels from VPN 3000 Series Concentrators to the ASA	Maps the logging security levels in the VPN 3000 Concentrator Manager to the ASA.

Related Documentation

This guide is a companion to the following user guides:

- *Cisco ASA 5500 Series Hardware Installation Guide*
- *Cisco ASA 5500 Series Quick Start Guide*
- *Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series*
- *Cisco ASA 5500 Series Release Notes*
- *Cisco ASDM Release Notes*
- *Cisco Security Appliance Command Line Configuration Guide*
- *Cisco Security Appliance Command Reference*

Conventions

This document uses the following conventions:

Convention	Description
boldface font	User actions and commands are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font in the command-line interface (for example, **`vpnclient stat)`**.

Notes use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Cautions use the following conventions:

Caution Means *reader be careful*. Cautions alert you to actions or conditions that could result in equipment damage or loss of data.

As you configure and manage the system, enter data in the following formats unless the instructions indicate otherwise:

Type of Data	Format
IP Addresses	IP addresses use 4-byte dotted decimal notation (for example, `192.168.12.34`); as the example indicates, you can omit leading zeros in a byte position.
Subnet Masks and Wildcard Masks	Subnet masks use 4-byte dotted decimal notation (for example, `255.255.255.0)`. Wildcard masks use the same notation (for example, `0.0.0.255)`; as the example illustrates, you can omit leading zeros in a byte position.
MAC Addresses	MAC addresses use 6-byte hexadecimal notation (for example, `0001.03cf.0238).`
Hostnames	Hostnames use legitimate network hostname or end-system name notation (for example, `VPN01)`. Spaces are not allowed. A hostname must uniquely identify a specific system on a network.
Text Strings	Text strings use upper- and lower-case alphanumeric characters. Most text strings are case-sensitive (for example, simon and Simon represent different usernames). In most cases, the maximum length of text strings is 48 characters.
Port Numbers	Port numbers use decimal numbers from `0` to `65535`. No commas or spaces are permitted in a number.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://cisco.com/univercd/cc/td/doc/pcat/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Feature Differences

This document helps current users of the VPN 3000 Series Concentrator migrate to the security appliance. The document highlights differences between the two devices and their software. For a full description of the security appliance features, please see the documents in the following list:

- *Cisco ASA 5500 Series Quick Start Guide*
- *Cisco Security Appliance Command Line Configuration Guide*
- *Cisco Security Appliance Command Reference*
- *Cisco ASA 5500 Series Release Notes*
- *Cisco ASA 5500 Series Hardware Installation Guide*
- *Cisco ASA 5500 Series Product CD*
- *Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series*
- *Cisco ASDM Online Help*
- *Cisco ASDM Release Notes*

The security appliance implements most of the features of the VPN 3000 Series Concentrator, but in some instances, the way you configure and use those features differs from what you have been accustomed to on the VPN 3000. This chapter lists some specific ways that the security appliance software differs from that of the VPN 3000 Series Concentrator. Appendix A, "Mapping Topics from VPN 3000 Series Concentrators to ASDM," lists the differences between the graphical user interfaces: VPN 3000 Concentrator Manager and the Adaptive Security Appliance Device Manager.

Mapping Features from the VPN 3000 Concentrators to ASA

Table 1-1 summarizes the mapping of the VPN 3000 Series Concentrator features to those available on ASA.

Table 1-1 Feature Map

Feature Name	VPN 3000	ASA
L2TP, L2TP over IPSec, and PPTP support	Supports L2TP, L2TP over IPSec, and PPTP features.	Does not include L2TP, L2TP over IPSec, or PPTP features.
Default encryption algorithm	3DES is the default for all crypto operations. No licensing is required for any crypto algorithm.	DES is the "base" encryption algorithm; 3DES and AES require "add-on" licenses.

Table 1-1 Feature Map (continued)

Feature Name	VPN 3000	ASA
IKE negotiations	The IKE Phase 1 ID is either a group name (receive only), an IP address, or a certificate DN. The transmitted Phase 1 ID is based on whether the VPN 3000 Concentrator is doing preshared key or certificate negotiation.	ASA supports multiple transforms for IKE Phase 2 and can send multiple proposals for IKE Phase 1. The IKE Phase 1 ID has more options, and it is configurable.
Default Setting of Phase 2 Data Integrity	The default Phase 2 Data Integrity setting is MD5.	The default setting for the Phase 2 Data Integrity value is “off”, for compatibility with previous versions of PIX and IOS. When configuring the security appliance to interoperate with a VPN 3000 Concentrator, you might need to enable Phase 2 data integrity.To *ensure* that IPSec data is authenticated via one of the hashing algorithms (SHA1 or MD5), the network administrator must turn on Phase 2 Data Integrity. To enable Phase 2 Data Integrity, turn on SHA1 or MD5 in the transform sets associated with the crypto maps you are using by following the steps in the section NAME, following this table. These commands enable SHA/HMAC-160 as the hash algorithm.
Low memory actions	Memory red condition prevents new connections when low on memory.	Prevents new connections when the device is out of memory. No “memory red” condition exists.
“Nice Reboot” configuration	Supports the “Nice Reboot” feature, which prevents the VPN 3000 Concentrator from rebooting until some applications have appropriately cleaned up. In the case of IKE, the Concentrator does not reboot until all tunnels are down.	“Nice Reboot” feature works the same as in the VPN 3000, but it is configured differently. First, configure the reboot to wait for the subsystems to clean up before rebooting. Then configure IKE to be notified of the reboot and to allow the reboot when all tunnels are down.

Table 1-1 Feature Map (continued)

Feature Name	VPN 3000	ASA
Hub-and-spoke configuration support	Supports a hub-and-spoke configuration.	Supports a hub-and-spoke configuration that lets encrypted traffic enter, be decrypted, and leave, in the clear, the same interface after firewall rules have been applied. Such "Client U-Turn" remote access connections can terminate on the outside interface of the security appliance, allowing Internet-destined traffic from remote-access user VPN tunnels to leave on the same interface as it arrived, after firewall rules have been applied.
Denial of Service (DoS) attack protection	To prevent a DoS attack, you can block Aggressive Mode. You can also disable DHCP relay.	To prevent a DoS attack, you can block Aggressive Mode.
CLI	Menu-driven selection. The primary interface with the product is the GUI.	PIX/IOS-like statement syntax.
Packet inspection	The VPN 3000 Concentrator does not inspect data going through it.	Because ASA is a firewall, it examines all data and does some level of intelligent inspection.
Configuring users	Users are configured under User Management.	Users are configured under Device Administration.
AIP SSM (Advanced Inspection and Prevention Security Services Module)	Not available	The AIP SSM features available depend on the ASA model.
Logging	Allows 13 severity levels of event logging.	Supports two logging mechanisms: • syslog, with levels 1through 7. This is equivalent to the VPN 3000 event logging function. • dbgtrace, a troubleshooting interface with limited reporting capabilities; for example, dbgtrace displays only to the console. dbgtrace has logging levels 1 through 11, plus 254 and 255. (See Appendix B, "Mapping Debug/Event Levels from VPN 3000 Series Concentrators to the ASA" for an explanation of these levels.)

Table 1-1 Feature Map (continued)

Feature Name	VPN 3000	ASA
Wildcard Masks	The VPN 3000 Concentrator uses wildcard masks, which are of the 0.0.0.255 variety as well as network masks, which are the inverse of wildcard masks in that they are of the 255.255.255.0 variety. VPN 3000 filters and downloadable ACLs are wildcard-based.	Wildcard masks do not work on the security appliance, which expects network masks in all cases. • When migrating from a VPN 3000 Concentrator to security appliance, network managers must configure security appliance crypto and interface ACLs with netmasks, not wildcards. • Existing VPN 3000 RADIUS DACL configurations must be modified to netmasks. • Mixed VPN 3000 and security appliance deployments, when downloading ACLs from RADIUS require some amount of segmentation, so that the VPN 3000 gets the DACLs with the wildcards, and the security appliance gets the DACLs with the netmasks.
Session timeout	Once some applications establish a TCP connection, they can stay up indefinitely without passing data. The VPN 3000 Concentrator tolerates this, but the security appliance does not.	ASA looks at TCP connections to make sure they active. If they are inactive for a configurable period of time, ASA tears down the TCP connection, which is comparable to terminating tunnels that have been unused for a long time. security appliance times out these sessions without indicating a reason. Thus, the application must reestablish the session to continue.

Table 1-1 Feature Map (continued)

Feature Name	VPN 3000	ASA
PKI and X.509 Certificate Support	No concept of trustpoints.	Major philosophical shift, as well as many syntax changes: • New concept of trustpoints and the way certificates are associated with trustpoints. • Supports IOS-based PKI functions, with the addition of VPN 3000 PKI features.
	RSA keys can be up to 2K in length.	For encrypt/decrypt operations, the security appliance can process RSA keys up to 4K in length.
	Supports VPN client authentication using X.509 certificates.	X.509 certificates support includes support for n-tier certificate chaining (for environments with a multi-level certificate authority hierarchy) and manual enrollment (for environments with offline certificate authorities). This release also supports the new certificate authority introduced in Cisco IOS, a lightweight X.509 certificate authority designed to simplify roll-out of PKI-enabled site-to-site VPN environments.
WebVPN	Configurable, available on all models. Offers features available on the latest Release 4.7 VPN 3000 Concentrator sustaining release, including: • SSL VPN Client • Cisco Secure Desktop • Citrix • NTLM authentication • PDA support.	• Support for WebVPN is equivalent to that available on the VPN 3000 Series Concentrator Release 4.1.7. • WebVPN is not available on PIX hardware.
Licensing	No license required.	Depending on the hardware platform, you can add separate, optional licenses to the base license to gain access to additional features. You can mix and match licenses, as appropriate for the hardware platform. See Appendix A of the *Cisco Security Appliance Command Line Configuration Guide* for details.

Table 1-1 Feature Map (continued)

Feature Name	VPN 3000	ASA
AAA	Uses the concepts of base group, groups, and users.	• ASA has two default tunnel groups, remote access and LAN-to-LAN, instead of the base group. There is only one default group policy. Default groups can no longer be used as a base group for certificate-based tunnels. • The functions of tunnel groups and group policies are split differently from the VPN 3000. Some attributes have moved to the tunnel group. These attributes cannot be configured on an external AAA server. The attributes that are not available in external groups are: – strip-realm – peer-id-validate – authorization-required – authorization-dn-attributes – authentication server type selection – authorization server type selection – radius-with-expiry
	Supports hybrid server groups (that is, servers in a group can be of different types).	Uses the concept of server groups. All servers in a server group must be of the same type.
	No fallback mechanism.	New fallback mechanism, including fallback to LOCAL if the named server is unavailable.
	No accounting for management traffic.	Richer administrative AAA features, including accounting for management traffic.
	RADIUS accounting data goes to a single server.	Supports simultaneous RADIUS accounting. You can specify whether accounting messages are sent to a single server (single mode) or sent to all servers in the group (simultaneous mode).
IPSec	Does not support tunneled ESP (ESP within an ESP tunnel).	Supports tunneled ESP.

Table 1-1 Feature Map (continued)

Feature Name	VPN 3000	ASA
Object Groups	Not used. Instead, the VPN 3000 uses network lists to make configuration easier.	Uses object grouping to simplify access list creation and maintenance.
Group attribute: Group Lock	The Group Lock feature is either enabled or disabled. When enabled, the VPN 3000 checks whether the Group Name used in the VPN Client to establish the connection is the same as the Group Name the user was assigned to. If they are not the same, the connection is dropped. If they are the same, the connection is allowed.	In ASA, the group-lock attribute is part of a group policy, and the value the parameter takes is the actual name of a tunnel group. When group-lock exists in a group policy, the ASA checks during a connection to see whether the Group Name used in the VPN Client is the same as the tunnel-group name found in the group-lock attribute.
Load balancing	Supported for remote sessions initiated with the Cisco VPN Client (Release 3.0 and later), the Cisco VPN 3002 Hardware Client (Release 3.5 or later), or the Cisco PIX 501/506E when acting as an Easy VPN client. Load balancing works with both IPSec clients and WebVPN sessions.	Available only on ASA5520 and ASA5540 systems. Not available for PIX hardware or for ASA 5510 systems.
Modes	No conceptual equivalent	• Supports virtual contexts and transparent versus routed modes. • VPN works only in single routed mode, except that you can have one management session to an ASA in transparent mode.

Table 1-1 Feature Map (continued)

Feature Name	VPN 3000	ASA
Quality of Service (QoS)	Configurable on all models.	Configurable only on ASA 5520 and ASA 5540 models. Not available for PIX hardware.
	Provides bandwidth policing to a maximum rate. Traffic that exceeds the maximum rate is dropped.	You can apply rate-limiting (policing) to all traffic, tunneled or non-tunneled, but you cannot apply rate limiting to priority-classed traffic. The ASA transmits traffic that exceeds the maximum rate, but throttles it to the maximum rate.
	• Guarantees a minimum bandwidth rate for tunneled traffic to assure that no one user can overwhelm the line rate at the interface and starve any other user. • Allows "stealing" of any unused bandwidth under reservation.	Bandwidth reservation is not supported. There is no minimum bandwidth guarantee.
	No low-latency queueing.	• Uses low-latency queueing (LLQ), so you can prioritize certain traffic types through the device. LLQ is *not* rate-limited. • All traffic other than LLQ traffic is considered "best effort." This traffic gets best-effort service after all LLQ traffic has been serviced, up to the depth of the best-effort queue. If the best-effort queue is full, any additional best-effort traffic is dropped.
	Applies only to tunneled traffic and is most commonly applied to the public interface.	You can configure QoS based on either tunnel-group information or ACLs.

Table 1-1 Feature Map (continued)

Feature Name	VPN 3000	ASA
Unlocking firewall function to allow VPN	Not applicable in VPN 3000.	No unlocking needed. After you enable ISAKMP on an interface, the security appliance can negotiate tunnels.
Filters/ACLs	Filters consist of rules that are applied to traffic in the order the rules are arranged on the filter. If a packet matches all the parameters specified in the rule, the system takes the action specified in the rule. If at least one rule parameter does not match, it applies the next rule; and so on. If no rule matches, the system takes the default action specified in the filter. • WebVPN uses filters to control access to specified URLs. • You can configure filters on a VPN Concentrator or on an external RADIUS server for use on the VPN 3000 Concentrator. Configuring a filter involves two steps: • Configuring the basic filter parameters (name, default action, etc. • Assigning rules to a filter. You apply filters to interfaces. These are the most important filters for security, because they govern all traffic through an interface. You also apply filters to groups and users and thus govern *tunneled* traffic through an interface.	• ACLs govern all traffic. • The Cisco ASA 5500 series security appliance supports outbound ACLs and time-based ACLs (building on existing inbound ACL support). Administrators can apply access controls as traffic enters an interface or exits an interface. Time-based access control lists provide administrators greater control over resource usage by defining when certain ACL entries are active. New commands let administrators define time ranges, and then apply these time-ranges to specific ACLs. • You can enable or disable specific ACL entries by appending an “active” or “inactive” keyword to those entries (rules without a keyword are active). This troubleshooting tool can facilitate fine-tuning ACLs.

Enabling Phase 2 Data Integrity for ASA

To *ensure* that IPSec data is authenticated via one of the hashing algorithms (SHA1 or MD5), the network administrator must turn on Phase 2 Data Integrity. To enable Phase 2 Data Integrity, turn on SHA1 or MD5 in the transform sets associated with the crypto maps you are using by following these steps. These commands enable SHA/HMAC-160 as the hash algorithm.

Note In the following descriptions, the terms IKE and ISAKMP are equivalent. VPN documentation tends to use IKE, and ASA tends to prefer ISAKMP (as does PIX). In ASA, all the commands use **isakmp**.

Step 1 Enable SHA/HMAC-160 for the transform-set you are using:

crypto ipsec transform-set *transform-set-name* **esp-3des esp-sha-hmac**

Step 2 Bind the transform set to the crypto map you are using:

crypto map *map-name seq-num* **set transform-set** *transform-set-name*

The following example enables SHA1 for a transform set named ttt, and binds it to a crypto map named abc. The sequence number (seq-num) is 1.

```
hostname(config)# crypto ipsec transform-set ttt esp-3des esp-sha-hmac
hostname(config)# crypto map abc 1 set transform-set ttt
hostname(config)#
```

Introducing the ASA System

This chapter addresses some of the major differences between the VPN 3000 Concentrator and the ASA, specifically for VPN. It includes the following sections:

Brief Overview of Security Policy Features

The ASA system combines Cisco's most powerful firewall, VPN, and intrusion protection features in a best-of-breed security appliance.

- The ASA provides a majority of the software features supported in the VPN 3000 Concentrator, including WebVPN.
- The ASA hardware of the provides faster interfaces (10/100/1000), an additional interface (4), and is expandable, containing a slot for additional security services.
- The operating system uses IOS-like CLI commands, which adds power and flexibility, improves on the menu-based command-line interface of the VPN 3000 Concentrator, and adds the ability to use scripts to automate configuration and monitoring processes. The CLI commands have been updated to support functionality transported into the ASA from the VPN Concentrator and there are many new commands specifically designed for VPN features. For information on CLI commands, see the *Cisco Security Appliance Command Reference*.
- The ASA performance exceeds that of the VPN 3000 Concentrator.
- The ASA provides for scalability and investment protection: multiple services are available in the same device, expansion is possible in the future with additional interfaces or services.
- The device management software provides a multicontext management interface to the ASA system.

The following sections describe the key concept differences between the ASA and the VPN 3000 Concentrator.

User Management Differences

Groups and users are core concepts in configuring the security of the VPN 3000 Concentrator. The attributes assigned to groups and users determine a user's access rights. In the VPN 3000, users are by default members of the *base group*. Otherwise, they are members of a customized group. The base group or customized group determines the attribute settings of each user. In the VPN 3000, the base group parameters are most likely to be common across all groups and users. As you configure a group, you can specify that it inherit parameters from the base group; a user can also inherit parameters from the group.

The ASA preserves the notion of groups and includes all of the group attributes provided by the VPN 3000 Concentrator. However, its implementation differs markedly. The ASA access rights to a user as follows:

1. Assigns access rights specified in the user profile.
2. Assigns the remaining rights from the group policy obtained from the first successfully received from the following sequence:
   a. Group policy named in the user profile.
   b. Otherwise, the group policy assigned to the tunnel group.
   c. Otherwise, the default group policy.

The user automatically inherits any attributes not explicitly set in the user profile.

The user attributes also support a null "none" value that you can set to ignore the associated setting in the group policy. Thus, the explicitly set user attribute settings and the remaining settings from the group policy determine the user's access rights to the VPN.

ASA Tunnel Groups, Group Policies, and Users

Note ASA also includes the concept of object groups, which are a superset of network lists. Object groups let you define VPN access to ports as well as networks. Object groups relate to ACLs rather than to group policies and tunnel groups.

ASA Tunnel Groups

Tunnel groups contain a small number of attributes germane to creating the tunnel itself. These attributes include a pointer to a group policy that defines further connection terms. The ASA includes a default tunnel group for LAN-to-LAN connections named DefaultL2LGroup and one for remote access connections named DefaultRAGroup. You can modify the default tunnel groups and group policy, but you cannot delete them.

Tunnel groups are local to the ASA, and are not configurable on external servers.

Tunnel groups specify the attributes identified in the following sections.

Tunnel group name

Clients select a tunnel group by its name.

- IPSec clients using preshared keys to authenticate pass the group name to the ASA.
- IPSec clients using certificates to authenticate pass this name as part of the certificate distinguished name. The ASA extracts the name from the certificate.
- IPSec clients can code the tunnel group name into the username in the format *username@TunnelGroup*. If the client does not specify the tunnel group in the username, the ASA recalls the tunnel group name used in IKE negotiations.

Connection type

A tunnel group may be either of the following connection types:

- Remote access IPSec.
- LAN-to-LAN IPSec.

Authentication, authorization, and accounting servers

The ASA uses the AAA servers for the following purposes:

- To authenticate users.
- To obtain information about services users are authorized to access.
- To store accounting records.

A server group can consist of one or more servers.

A default group policy for the connection

This is the group policy whose attributes the ASA uses as defaults when authenticating or authorizing a tunnel user. The name of this group policy is DfltGrpPolicy, which you can edit but not delete.

A client address assignment method

This includes values for one or more of the following:

- DHCP servers or address pools that the security appliance assigns to clients.
- RADIUS authentication server group.
- Static IP addresses used by the clients.

IPSec connection parameters

IPSec parameters include the following:

- A client authentication method: preshared keys or certificates.
- ISAKMP keepalive settings.
- Values for defining authorization usernames.

Group Policies

A group policy is a set of user-oriented attributes for IPSec connections. The tunnel group refers to a group policy that sets terms for user connections after the tunnel is established. Group policies let you apply whole sets of attributes to a user rather than having to specify each attribute individually for each user.

By default, users inherit all user attributes from the assigned group policy. But the ASA also lets you modify individual attributes of group policies for individual users. There is one default group policy, which is named DfltGrpPolicy. You can modify this group policy, but you cannot delete it. You can also create one or more group policies specific to your environment.

In ASDM, use the **Configuration > Features > Device Administration > User Accounts** panel to assign a group policy to users or to modify a group policy for specific users. In the CLI, use the group-policy commands in global configuration mode.

Group policies include the following attributes:

Identity

Identifies the name of the group policy and its type.

- Name—must be unique.
- Type—Internal or External. Internal means that this group policy specifies authentication through a database. External means that this group policy specifies authentication through an external server such as RADIUS.

Tunneling protocols

Configures the tunneling protocols, such as IPSec or WebVPN that this group policy provides.

Filters

Specifies the filter to use for this group policy. Filters, referred to as *access control lists* in the ASA, are rules that determine whether to allow or reject tunneled data packets coming through the ASA, based on criteria such as source address, destination address, and protocol.

Connection settings

Specifies the following connection parameters:

- Access hours—Indicates the name of the selected access hours policy that this group policy uses.
- Simultaneous logins—Specifies the maximum number of simultaneous logins allowed for this group policy.
- Maximum connect time—Specifies the maximum user connection time in minutes.
- Idle timeout values—Specifies the amount of time that a user can be idle in minutes. If there is no communication activity on a user's connection in this period, the system terminates the connection. This value does not apply to WebVPN users.

Defining servers

Configures DNS, WINS, and optionally, the DHCP scope, as follows:

- DNS—Specifies the DNS servers to use. You can specify primary and secondary DNS servers.
- WINS—Specifies the WINS servers to use. You can specify primary and secondary WINS servers.
- DHCP Scope—Specifies the IP subnetwork the DHCP server uses to assign IP addresses to users of the group policy you are configuring.

IPSec settings

Configures the following parameters.

- ReAuth on Rekey—Enables/disables reauthentication when IKE re-key occurs. If reauthentication is enabled, the system prompts a user to enter an ID and password during Phase 1 IKE negotiation and also prompts for user authentication whenever a rekey occurs.
- IP Compression—Shrinks data by replacing repeating information with symbols that use less space.
- Perfect Forward Secrecy—Ensures that the key for a given IPSec SA was not derived from any other secret (such as some other key).
- Tunnel Group Lock—Enables locking of a specified tunnel group, which means that members of the tunnel group are restricted to remote access through this tunnel group only.
- Client Access Rules (access control lists)—configures up to 25 client access rules, which specify values for the priority of the rule, action allowed (permit or deny), and the VPN client type and version.

Client configuration

Configures the following parameters for remote-access VPN clients.

- Banner—Lets a network administer specify and edit text for the banner that the remote-access users see when connecting to the system.
- Default domain—Specifies the name of the default domain that the system passes to the IPSec client, for the client's TCP/IP stack to append to DNS queries that omit the domain field. This domain name applies only to tunneled packets.
- Split tunneling—Configures how to make tunneling decisions (see "Configuring Split Tunneling and Network Lists").
- Cisco client settings—Configures parameters specific to the Cisco VPN client, such as password storage on the client system, IPSec over UDP, UDP port parameter, and so on.

Client firewall

Configures client firewall options, including what type of firewall (if any) and the firewall policy for that firewall.

HW client settings

Configures the following EzVPN client settings for the group policy.

- Secure unit authentication—Enables/disables requirement for interactive client authentication. This requires the EzVPN client to authenticate with a username and password entered manually each time it initiates a tunnel.
- Individual user authentication—Enables/disables requirement for individual user authentication for users behind the EzVPN clients in the tunnel group using the group policy.
- User authentication idle timeout—Specifies the time to wait before terminating the connection when there is no communication activity on the connection.
- IP Phone Bypass—Lets Cisco IP phones bypass the interactive individual user authentication processes.
- LEAP Bypass—Enables/disables LEAP packets traveling from Cisco wireless devices. LEAP (Lightweight Extensible Authentication Protocol) Bypass lets LEAP packets from devices behind a EzVPN client travel across a VPN tunnel prior to individual user authentication.
- Allow Network Extension mode—Enables/disables restriction of network extension mode on the EzVPN client. Network extension mode is required for the EzVPN client to support IP phone connections.

WebVPN

Configures the following parameters for WebVPN connections.

- WebVPN functions, such as enabling URL entry, file server access, entry, browsing, and so on.
- Content filtering—Blocks or removes the parts of websites that do the following:
  - Use Java or Active X
  - Use scripts
  - Display images
  - Deliver cookies
- Homepage—Determines the home page.
- Port forwarding—Sets the port forwarding parameters.
- Server and url lists—Specifies whether to inherit the list of servers and URLs from the default group policy, to select an existing list, or create a new list.
- WebVPN ACL ID—Specifies the identifier of the WebVPN access control list to use.

User Accounts

This is where you assign a group policy to a user. You can also make exceptions for a user to one or more values in a group policy.

Attributes include:

- General
  - Username—Specifies the name of the user to whom the parameters in the user account apply.
  - Password—Specifies the unique password for this user.
  - Privilege Level—Specifies the privilege level assigned to the user account. The range is 0 (lowest) to 15 (highest). The authorization server uses Level 0 to permit VPN access, and the ASA uses Level 15 for the highest administrator access to the CLI commands. You can enter the **show running-config all privilege** CLI command to list all commands and their associated privilege levels.
- VPN Policies
  - Group Policy—Identifies which group policies are available to the user.
  - Tunneling Protocols—Specifies the tunneling protocols that this user can use: IPSec or WebVPN.
  - Filter parameters (ACLs)—Specifies the filter to use. Filters are rules that determine whether to allow or reject tunneled data packets coming through the security appliance based on criteria such as source address, destination address, and protocol.
  - Tunnel Group Lock parameters—Specifies the tunnel group lock that applies to a user. A tunnel group lock restricts users to specific tunnel groups.
  - Store Password on the client system—Controls whether to store the login password on the client system.
  - Connection Settings—Controls the following options: access hours, simultaneous logins, maximum connect time, and idle timeout.
  - Dedicated IP address—Specifies a static IP address and subnet mask.
- WebVPN Policies (see the "Group Policies" section)

PKI Implementation on ASA

The implementation of PKI on the ASA differs from the VPN 3000 Concentrator implementation. The main concept of the PKI model on ASA is the trustpoint. Trustpoints have the following characteristics:

- Trustpoints have a one-to-one relationship with local identities.
- Trustpoints have a many-to-one relationship with CA identities.
- Trustpoints specify enrollment request content, defaults, and method of enrollment.
- Trustpoints specify CRL configuration parameters.

To configure trustpoints in the CLI, the ASA provides the **crypto ca trustpoint** command. This command contains a subset of IOS options and additional parameters for existing VPN 3000 features migrating to the ASA. For information on this command and its subcommands, see *Cisco Security Appliance Command Reference*. You can configure all the PKI features in ASDM (see "Enrolling for Digital Certificates" in this guide for more information).

Table 2-1 lists the other new PKI commands.

Table 2-1 New PKI Commands for the ASA

Command Sets	Action
crypto key	Generates key pairs: RSA or DSA.
crl configure	Under **crypto ca trustpoint**, this command enters **crl** configuration mode and lets you configure CRL parameters.
crl	Enables you to configure a large number of parameters carried over from the VPN 3000 Concentrator.
crypto ca authenticate	Obtains by downloading or pasting a certificate from a certification authority.
crypto ca enroll	Initiates enrollment with the CA.
crypto ca import (not a new command)	Installs a certificate received from a CA in response to a manual enrollment request.
crypto ca crl	Requests a certificate revocation list based on the settings of the specified configuration.
crypto ca certificate map	Maintains a prioritized list of certificate-mapping rules. This command provides for certificate-group matching in the VPN 3000 Concentrator.
tunnel-group-map	Configures policy and rules by which certificate-based IKE sessions are mapped to tunnel groups.

ASDM and WebVPN Sessions per Interface

ASA supports either WebVPN or an ASDM administrative session on an interface, but not both simultaneously. To use ASDM and WebVPN at the same time, configure them on different interfaces.

Getting Started

This chapter provides an overview of the VPN 3000 Concentrator's Quick Configuration program and describes where to go in the ASDM to configure the counterpart features. Following the outline of configuration tasks, this chapter lists the information needed to run the VPN wizard to configure site-to-site and remote access tunnels.

Quick Configuration Tasks and Counterparts in ASDM

Table 3-1 describes the following configuration tasks and where to perform these tasks in ASDM.

- Configuring IP interfaces
- Configuring system information
- Configuring tunneling protocols and options
- Configuring an address management method
- Configuring authentication
- Configuring an internal server user database
- Configuring IPSec groups
- Configuring an administrator password

Table 3-1 Getting Started Tasks

VPN 3000 Quick Configuration Tasks	ASA Counterpart
Configuring IP interfaces Enter the IP address and subnet mask for private and public ethernet connections. Optionally, enter addresses for the external interface. • Enable/disable • DHCP Client/system name • Static IP addressing (IP addr/subnet mask) • Type of interface (public or private) • MAC address • Filter • Speed • Duplex • MTU	Go to **Configuration > Features > Interfaces**. • Add/Edit – Select Hardware Port – Check Enable Interface • Enter: – VLAN ID – Sub-interface ID – Interface Name – Security Level – Source of IP Address: Static IP or DHCP – IP Address – Subnet Mask – MTU • Click **Properties...** – Select Duplex type: Full, Half, Auto – Select Speed 10, 100, Auto • Optionally enable traffic between two or more interfaces configured with the same security levels.
Configuring system information • System hostname • Time and date • DNS server information (IP address, Internet domain name, default gateway)	Go to **Configuration > Features > Device Administration > Administration > Device**. • Enter host name and domain name. • Go to **Device Administration > Administration > Clock** to enter time and date. • Go to **Configuration > Features > Properties > DNS Client**. – Add Servers (up to 6). – Enter timeout in seconds. – Enter number of retries. – Enable DNS lookup on interfaces.
Configuring tunneling protocols and options • PPTP -- encryption option • L2TP -- encryption option • IPSec (allows remote access only. Can't do site-to-site through QC)	To define Tunnel Groups go to **Configuration > Features > VPN > General > Tunnel Group**. Two default tunnel groups for IPSec: • DefaultL2LGroup for LAN-to-LAN • DefaultRAGroup for Remote Access

Table 3-1 Getting Started Tasks

VPN 3000 Quick Configuration Tasks	ASA Counterpart
Configuring address management method • Client specifies its own IP address. • Assign IP addresses per user (use auth server). • Use DHCP (specify server address or name). • Configure a pool (start/end ranges).	Go to **Configuration > Features > VPN > IP Address Management > Assignment**. Choices: • Use address from authentication server. • Use DHCP. • Use internal address pools. • Configure IP address pools under **Configuration > Features > VPN > IP Address Management > IP Pools**.
Configuring authentication • Choose a server type: internal, RADIUS, NTDomain, SDI, Kerberos/Active Directory. • Fill in information for selected authentication server. Each has its own screen.	Go to **Configuration > Features > Properties > AAA Setup**. • Add server groups. • Add servers to server groups. • Configure authentication prompts.
Configuring internal server user database Enter user information: • User name • Password • Verify password • IP address (if per-user address assignment) • Subnet mask	Go to **Configuration > Features > Device Administration > Administration > User Accounts**. Add user account and enter information: • Under Identity: Username Password Confirm Password Privilege Level • Under VPN Policy (specify or check inherit if from group policy) Group Policy (previously defined) Tunneling Protocols Filter Tunnel Group Lock Store Password on Client System Connection Settings Dedicated IP address (optional)
Configuring IPSec group • Group name • Password • Verify	Go to **Configuration > Features > VPN > General > Tunnel Group**. Add tunnel group of IPSec type.

Table 3-1 Getting Started Tasks

VPN 3000 Quick Configuration Tasks	ASA Counterpart
Configuring administrator password	Go to **Configuration > Features > Device Administration > Administration > Password**.
Testing the VPN Connection steps	

Configuring a VPN Tunnel Using the VPN Wizard

The VPN wizard lets you configure a site-to-site or remote access VPN tunnel from the ASA to either another VPN device or a remote client user. You can use the wizard to define new VPN configurations only. Once you have configured a VPN tunnel using the wizard, you can edit it by using the ASDM features, especially in the **Configuration > Features > VPN** section.

Gathering Information

Before you launch the VPN wizard, gather the information needed to configure the VPN tunnel. To do so, use the section that names the tunnel type you want to configure.

- Site-to-Site VPN Tunnels
- Remote Access Using Locally Stored User Accounts
- Remote Access Using AAA Server Group for Client Authentication

Site-to-Site VPN Tunnels

When you configure a site-to-site VPN tunnel using the VPN wizard, you need to have the following information before you begin.

Note When recording these values, take note of the associated number. These numbers mirror the step numbers that appear in the VPN Wizard that you run after assembling this data.

1. VPN Tunnel Type

   Interface for the site-to-site VPN tunnel (for example, “inside” or “outside”)—Before you can configure a VPN tunnel, you configure interfaces for the security appliance. When you configure the tunnel, you select an interface to associate with the VPN tunnel you are configuring.

2. Remote Site Peer

   IP address of peer device at the other end of the tunnel

   Optional name for the tunnel group (which defaults to the peer’s IP address)

   Authentication type (preshared key or digital certificate). You also need one of the following:

   - If preshared, the name of the key.
   - If digital certificate, the certificate signing algorithm (RSA or DSA), and the name of the trustpoint.

     See “Key Pairs” for the differences between the RSA and DSA algorithm.

A trustpoint is a representation of a CA or identity pair. A trustpoint contains the identity of the CA, CA-specific configuration parameters, and an association with one enrolled identity certificate.

Note If you choose the digital certificate authentication type, configure the trustpoints (see the "Creating the Trustpoint" section on page 4-4) before running the VPN wizard.

3. IPSec Phase 1 Internet Key Exchange Security Association policy to be used to negotiate the tunnel, which consists of the following:
   - Encryption algorithm for IPSec VPN tunnel, which must be the same for both devices—DES, 3DES, AES-128, AES-192, or AES-256. The default is DES.
   - Authentication algorithm for the IPSec VPN tunnel, which must be the same for both devices—MD5 or SHA. The default is SHA.

     Diffie Hellman Group, which must be the same for both devices—group 1, group 2, group 5, or group 7. The default is group 2.
4. IPSec Phase 2 Encryption and Authentication policy to be applied to the VPN tunnel. The parameters and options consist of the following:
   - Encryption algorithm for IPSec VPN tunnel, which must be the same for both devices—DES, 3DES, AES-128, AES-192, or AES-256. The default is DES.
   - Authentication algorithm for the IPSec VPN tunnel, which must be the same for both devices—MD5 or SHA. The default is SHA.
5. Local Hosts and Networks—Hosts and networks at the local site of the IP connection. You have the following options for specifying the hosts and networks at the local site of the IP connection:
   - IP address. You need the following information if you choose this option:

     Interface name—The interface, such as "inside" or "outside," to which the host is connected.

     IP address—Any, the address of a specific local host, or a subnet. If you choose any, the IP address and subnet mask become 0.0.0.0.

     Subnet mask—Values range from 255.255.255.255 to 0.0.0.0.
   - Name of the host already present in the ASA configuration.
   - Group containing lists of networks or hosts to protect. You need the following information if you choose this option:

     Name of the host already present in the ASA configuration.

     Name of the group already present in the ASA configuration.

Note To configure host/networks group names, go to **Configuration > Features > Building Blocks > Hosts/Networks**.

6. Remote hosts and networks—Hosts and networks at the remote site of the IP connection.

   The options are the same as those for the local hosts and networks.

After preparing the information described in this section, go to "Running the VPN Wizard."

Remote Access Using Locally Stored User Accounts

Prepare the following information for a remote access VPN tunnel requiring login accounts to be stored in the ASA configuration:

Note When recording these values, take note of the associated number. These numbers mirror the step numbers that appear in the VPN Wizard.

1. VPN Tunnel Type

   Interface for the site-to-site VPN tunnel (for example, “inside” or “outside”)—Before you can configure a VPN tunnel, you configure interfaces for the security appliance. When you configure the tunnel, you select an interface to associate with the VPN tunnel you are configuring.

2. Remote Access Client

   Use the default setting (Cisco VPN Client, Release 3.x or higher, or other Easy VPN Remote product) to specify the type of VPN client supported for tunnels to this ASA. This release does not support other options.

3. VPN Tunnel Group Name and Authentication Method

   Name for the tunnel group to be used for both the remote clients and the ASA. The group name specifies common connection and client settings to be specified in the next steps.

   Authentication type (preshared key or digital certificate). You also need one of the following:

   - If preshared, the name of the key.
   - If digital certificate, the certificate signing algorithm (RSA or DSA), and the name of the trustpoint.

     See “Key Pairs” for the differences between the RSA and DSA algorithm.

     A trustpoint is a representation of a CA or identity pair. A trustpoint contains the identity of the CA, CA-specific configuration parameters, and an association with one enrolled identity certificate.

     Note If you choose the digital certificate authentication type, configure the trustpoints (Configuration > Features > Device Administration > Certificate) before running the VPN wizard.

4. Client Authentication, which provides a choice of one of the following options:

   - Authenticate using the local (internal) user database

     This option lets you populate the ASA configuration with user accounts.

   - Authenticate using an AAA server group

     This option let you select an AAA server group to handle client authentication. Go to this same step in the next section if you choose this option.

5. User Accounts

   If you chose “Authenticate using the local (internal) user database,” list the login name and respective password for each user to be inserted into the local database.

6. Address Pool

   You can select the name of an IP address pool already present in the ASA configuration or specify a new one. If you specify a new one, you need a new pool name, the associated IP address range, and optionally a subnet mask.

7. (Optional) Attributes Pushed to Client

   You can choose to push the following attributes to the VPN client when it connects:

   - IP addresses of primary and secondary DNS servers
   - IP addresses of primary and secondary WINS servers
   - Default domain name

8. IPSec Phase 1 Internet Key Exchange Security Association policy to be used to negotiate the tunnel, which consists of the following:

   - Encryption algorithm for IPSec VPN tunnel, which must be the same for both devices—DES, 3DES, AES-128, AES-192, or AES-256. The default is DES.
   - Authentication algorithm for the IPSec VPN tunnel, which must be the same for both devices—MD5 or SHA. The default is SHA.

     Diffie Hellman Group, which must be the same for both devices—group 1, group 2, group 5, or group 7. The default is group 2.

9. IPSec Phase 2 Encryption and Authentication policy to be applied to the VPN tunnel. The parameters and options consist of the following:

   - Encryption algorithm for IPSec VPN tunnel, which must be the same for both devices—DES, 3DES, AES-128, AES-192, or AES-256. The default is DES.
   - Authentication algorithm for the IPSec VPN tunnel, which must be the same for both devices—MD5 or SHA. The default is SHA.

10. (Optional) Address Translation Exemption and Split Tunneling

    Hosts and networks in the internal network to expose to authenticated remote users of the VPN. Specify none to expose the entire internal network to authenticated remote users in the tunnel, or specify the internal addresses to expose to them and leave Network Address Translation to hide the remainder. You have the following options for specifying the internal addresses of the hosts and networks at the local site of the IP connection:

    - IP address. You need the following information if you choose this option:

      Interface name—The interface, such as “inside” or “outside,” to which the host is connected.

      IP address—Any, the address of a specific local host, or a subnet. If you choose any, the IP address and subnet mask become 0.0.0.0.

      Subnet mask—Values range from 255.255.255.255 to 0.0.0.0.
    - Name of the host already present in the ASA configuration.
    - Group containing lists of networks or hosts to protect. You need the following information if you choose this option:

      Name of the host already present in the ASA configuration.

      Name of the group already present in the ASA configuration.

Note To configure host/networks group names, go to **Configuration > Features > Building Blocks > Hosts/Networks**.

Split Tunneling—enable to provide VPN users with unencrypted access to the Internet, or leave disabled.

Note If you enable split tunneling, the hosts identified above also serve as the split tunnel access list.

After preparing the information described in this section, go to "Running the VPN Wizard."

Remote Access Using AAA Server Group for Client Authentication

Prepare the following information for a remote access VPN tunnel requiring client authentication using a AAA server group:

Note When recording these values, take note of the associated number. These numbers mirror the step numbers that appear in the VPN Wizard.

1. VPN Tunnel Type

   Interface for the site-to-site VPN tunnel (for example, "inside" or "outside")—Before you can configure a VPN tunnel, you configure interfaces for the security appliance. When you configure the tunnel, you select an interface to associate with the VPN tunnel you are configuring.

2. Remote Access Client

   Use the default setting (Cisco VPN Client, Release 3.x or higher, or other Easy VPN Remote product) to specify the type of VPN client supported for tunnels to this ASA. This release does not support other options.

3. VPN Tunnel Group Name and Authentication Method

   Name for the tunnel group to be used for both the remote clients and the ASA. The group name specifies common connection and client settings to be specified in the next steps.

   Authentication type (preshared key or digital certificate). You also need one of the following:

   - If preshared, the name of the key.
   - If digital certificate, the certificate signing algorithm (RSA or DSA), and the name of the trustpoint.

     See "Key Pairs" for the differences between the RSA and DSA algorithm.

     A trustpoint is a representation of a CA or identity pair. A trustpoint contains the identity of the CA, CA-specific configuration parameters, and an association with one enrolled identity certificate.

     Note If you choose the digital certificate authentication type, configure the trustpoints (Configuration > Features > Device Administration > Certificate) before running the VPN wizard.

4. Client Authentication, which provides a choice of one of the following options:

   - Authenticate using the local (internal) user database

     This option lets you populate the ASA configuration with user accounts. Continue with Step 5 in the previous section if you choose this option.

- Authenticate using an AAA server group

  If you choose this option, select the name of an AAA server group you already added to the configuration or create a new one. The **Configuration > Features > Properties > AAA Setup** path lets you examine and manage the AAA server configuration. The Client Authentication panel in the VPN Wizard that provides these authentication options also provides a **New** button that lets you create a AAA server group. If you choose this option, be ready to give the group a name, choose an authentication protocol (RADIUS, TACACS+, SDI, NT, or Kerberos), specify the IP address of the server, choose the interface (such as "inside" or "outside," and specify the server secret key.

5. Address Pool

   You can select the name of an IP address pool already present in the ASA configuration or specify a new one. If you specify a new one, you need a new pool name, the associated IP address range, and optionally a subnet mask.

6. (Optional) Attributes Pushed to Client

   You can choose to push the following attributes to the VPN client when it connects:

   - IP addresses of primary and secondary DNS servers
   - IP addresses of primary and secondary WINS servers
   - Default domain name

7. IPSec Phase 1 Internet Key Exchange Security Association policy to be used to negotiate the tunnel, which consists of the following:

   - Encryption algorithm for IPSec VPN tunnel, which must be the same for both devices—DES, 3DES, AES-128, AES-192, or AES-256. The default is DES.
   - Authentication algorithm for the IPSec VPN tunnel, which must be the same for both devices—MD5 or SHA. The default is SHA.

     Diffie Hellman Group, which must be the same for both devices—group 1, group 2, group 5, or group 7. The default is group 2.

8. IPSec Phase 2 Encryption and Authentication policy to be applied to the VPN tunnel.
   The parameters and options consist of the following:

   - Encryption algorithm for IPSec VPN tunnel, which must be the same for both devices—DES, 3DES, AES-128, AES-192, or AES-256. The default is DES.
   - Authentication algorithm for the IPSec VPN tunnel, which must be the same for both devices—MD5 or SHA. The default is SHA.

9. (Optional) Address Translation Exemption and Split Tunneling

   Hosts and networks in the internal network to expose to authenticated remote users of the VPN. Specify none to expose the entire internal network to authenticated remote users in the tunnel, or specify the internal addresses to expose to them and leave Network Address Translation to hide the remainder. You have the following options for specifying the internal addresses of the hosts and networks at the local site of the IP connection:

   - IP address. You need the following information if you choose this option:

     Interface name—The interface, such as "inside" or "outside," to which the host is connected.

     IP address—Any, the address of a specific local host, or a subnet. If you choose any, the IP address and subnet mask become 0.0.0.0.

     Subnet mask—Values range from 255.255.255.255 to 0.0.0.0.

   - Name of the host already present in the ASA configuration.

– Group containing lists of networks or hosts to protect. You need the following information if you choose this option:

  Name of the host already present in the ASA configuration.

  Name of the group already present in the ASA configuration.

Note To configure host/networks group names, go to **Configuration > Features > Building Blocks > Hosts/Networks**.

Split Tunneling—enable to provide VPN users with unencrypted access to the Internet, or leave disabled.

Note If you enable split tunneling, the hosts identified above also serve as the split tunnel access list.

After preparing the information described in this section, go to "Running the VPN Wizard."

Running the VPN Wizard

To run the VPN wizard, follow these steps:

Step 1 Go to **Wizards > VPN Wizard**.

Step 2 Select the type of tunnel to set up: **Site to Site** or **Remote Access**.

Step 3 Select **Inside** or **Outside** next to the VPN Tunnel Interface.

Step 4 Click **Next** and follow the instructions in the VPN wizard. For more information, click **Help**.

Saving the Configuration

As you work, remember to save the changes to Flash memory to retain them, as follows:

- ASDM—Select **File > Save Running Configuration to Flash**.
- CLI—Enter the **wr mem** command.

Displaying the Configuration

You can enter either of the following commands to display the current configuration settings:

- FWSM# **show config**

  Enter this command to show the startup configuration saved to flash memory.
- FWSM# **show run**

  Enter this command to show the operating configuration.

Note The two commands are equivalent if you saved the configuration changes you made.

You can also type **show run ?** to display a detailed list of the show configuration commands you can enter to retrieve a more refined list.

Using ASDM to Learn the CLI

The ASDM **Options > Preferences** window provides a "Preview commands before sending to the device" option. If you enable this option, ASDM displays the equivalent CLI commands in the Preview CLI Commands window whenever you click **Apply**.

View the commands, click **OK**, and then click **Proceed** in the confirmation window to save the changes to the running configuration.

CHAPTER 4

Building Basic VPN Tunnels

The following sections show how to use CLI commands and ASDM to configure LAN-to-LAN and remote access tunnels, and use preshared keys or digital certificates to authenticate them:

Note ASDM comes with a complete online-help system. For field definitions on any panel, click **Help**.

For the complete syntax of the commands used in this chapter, see *Cisco Security Appliance Command Reference*.

Enrolling for Digital Certificates

This section describes how to enroll for a digital certificate using CLI commands and ASDM. Once enrolled, you can use the certificate to authenticate VPN LAN-to-LAN tunnels and remote access tunnels. If you intend to use only preshared keys to authenticate, you do not need to read this section.

Key Pairs

Each peer has a key pair containing both a public and a private key. These keys act as complements; any communication encrypted with one can be decrypted with the other.

Key pairs can be either RSA keys or DSA keys. Support for these two types of keys differs as follows:

- DSA keys cannot be used for SSH or SSL. To enable SSH or SSL access to a security appliance, use RSA keys.
- SCEP enrollment is only supported for the certification of RSA keys. If you use DSA keys, enrollment must be performed manually.
- For the purposes of generating keys, the maximum key modulus for RSA keys is 2048, and the maximum key modulus for DSA keys is 1024. The default size for either is 1024 bits.
- For signature operations, the supported maximum key sizes are 4096 bits for RSA keys and 1024 bits for DSA keys.

- You can generate a *general purpose* RSA key pair used for both signing and encryption, or *usage* RSA key pairs separated for each respective purpose, thus requiring two certificates for the corresponding identity. The default setting is general purpose. This topic does not apply to a DSA key pair because it is only for signing.

To configure a key pair for a certificate, you specify the labels to identify the key pair to be generated. The following sections show how to generate an RSA key pair with a default label using the CLI and a specified label using ASDM, and use the default settings for the other parameters.

Overview of Configuration Procedure

Enroll with a CA and get an identity certificate for authenticating tunnels as follows:

Note This example shows automatic (SCEP) enrollment.

1. Create a key pair for the identity certificate. The key pair can be either RSA or DSA. However, for automatic enrollment, you must use RSA keys. The instructions in the sections that follow show how to generate an RSA key pair.
2. Create a trustpoint. The name of the trustpoint in this example is newmsroot.
3. Configure an enrollment URL. The URL this example uses is http://10.20.30.40/certsrv/mscep/mscep.dll.
4. Authenticate the CA.
5. Enroll with the CA, which gets an identity certificate onto the ASA.

Using CLI Commands

You can enter the **show crypto key mypubkey DSA** or **show crypto key mypubkey RSA** command to display the current, operational key pairs.

The complete syntax of the CLI command to generate the key pair is as follows:

crypto key generate rsa [**usage-keys** | **general-keys**] [**label** *key-pair-label*] [**modulus** *size*]

For example, in global configuration mode, enter the following command to generate an RSA key pair with the default name <Default-RSA-Key>:

```
hostname(config)# crypto key generate rsa
INFO: The name for the keys will be: <Default-RSA-Key>
Keypair generation process begin. Please wait...
```

Using ASDM

Generate an RSA key pair using ASDM, as follows:

Step 1 Under the **Configuration > Features > Device Administration > Certificate > Key Pair** panel, click **Add**.

Step 2 Configure the information in the **Add Key Pair** dialog box:

a. **Name—**Click to use the default name, or type a name for the key pair(s). This example uses the name key1.

b. **Size** list—For an RSA key pair, the **Size** list displays the options: 512, 768, 1024, or 2048. The default size is 1024. This example accepts the default setting.

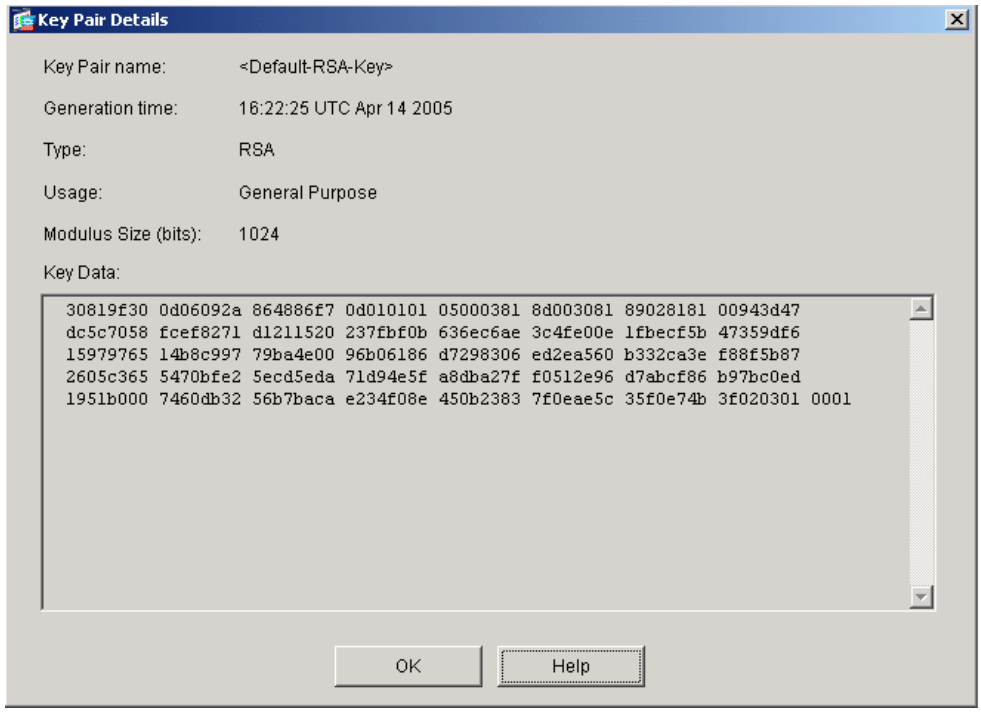
c. **Type** options—**Type** options are RSA and DSA. For this example, accept the default setting, RSA.

d. **Usage** options—(Applicable only if the Type is RSA.) The options are General Purpose (one pair for both signing and encryption) and Special (one pair for each respective function). For this example, accept the default setting (General Purpose).

Step 3 Click **Generate Now**.

Step 4 To view the key pair generated, click **Show Details**. ASDM displays information about the key pair. Figure 4-1 shows sample output.

Figure 4-1 Key-pair Details Display



Creating the Trustpoint

A trustpoint represents a CA/identity pair and contains the identity of the CA, CA-specific configuration parameters, and an association with one enrolled identity certificate. Refer to the section that names the interface you want to use to create a trustpoint.

Using CLI Commands

Use the **crypto ca trustpoint** CLI command to create a trustpoint. This command puts you in config-ca-trustpoint mode and lets you manage trustpoint information. Following this command, you need only two trustpoint commands: **enrollment url** and **subject-name**.

Follow these steps and use the syntax in the example commands:

Step 1 From global configuration mode, enter config-ca-trustpoint mode and create a new trustpoint. In this example, the name of the trustpoint is newmsroot.

```
hostname(config)# crypto ca trustpoint newmsroot
```

Step 2 To specify automatic enrollment (SCEP) to enroll with this trustpoint and configure the enrollment URL, use the **enrollment url** command. Then to specify the distinguished (X.500) name for the certificate, use the **subject-name** command. This is the person or system that uses the certificate. The DN field does support group matching. This example uses the common name (CN) and the organizational unit (OU).

```
hostname(config-ca-trustpoint)# enrollment url http://10.20.30.40/certsrv/mscep/mscep.dll
hostname(config-ca-trustpoint)# subject-name CN=Pat, OU=Techpubs
```

Step 3 (Optional) Display the trustpoint configuration, containing the default parameters and values.

```
hostname(config-ca-trustpoint)# show run all crypto ca trustpoint newmsroot
crypto ca trustpoint newmsroot
 crl nocheck
 enrollment retry period 1
 enrollment retry count 0
 enrollment url http://10.20.30.40/certsrv/mscep/mscep.dll
 fqdn hostname.ciscopix.com
 no email
 subject-name CN=Pat, OU=Techpubs
 serial-number
 no ip-address
 no password
 id-cert-issuer
 accept-subordinates
 support-user-cert-validation
 crl configure
  policy cdp
  cache-time 60
  enforcenextupdate
  protocol http
  protocol ldap
  protocol scep
```

Using ASDM

To create a trustpoint using ASDM, follow these steps:

Step 1 Under the **Configuration > Features > Device Administration > Certificate > Trustpoint > Configuration** panel, click **Add**.

Step 2 Configure the basic information in the **Add Trustpoint Configuration** dialog box. For all other parameters, accept the default values.

a. **Trustpoint Name** box—Type the trustpoint name in the **Trustpoint Name** box. For this example, the name is newmsroot.

b. **Enrollment URL** box—In the **Enrollment Settings** panel, under the **Enrollment Mode** group box, click the **Use automatic enrollment** option. Then type the enrollment URL in the box. For this example, type **10.20.30.40/certsrv/mscep/mscep.dll**.

Step 3 Configure the subject name using the common name (CN) and the name of the organizational unit (OU):

a. In the **Enrollment Settings** panel, select the key pair you configured for this trustpoint in the **Key Pair** list. For this example, the key pair is key1.

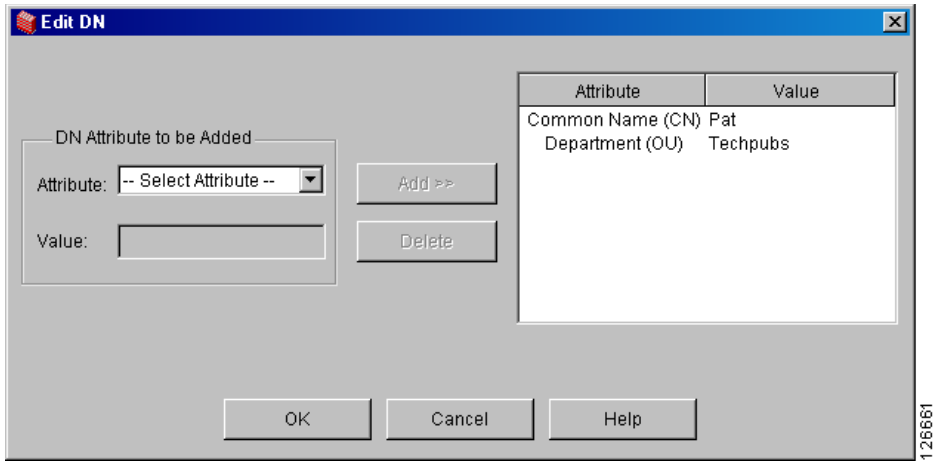
b. In the **Enrollment Settings** panel, click **Certificate Parameters**.

c. To add subject distinguished (X.500) name values, click **Edit** in the **Certificate Parameters** dialog box.

d. In the **Edit DN** box under **DN Attribute to be Added**, select an attribute in the **Attribute** list and type a value in the **Value** box. Then click **Add**. After entering the DN information, click **OK**.

For this example, first select **Common Name (CN)**, type **Pat** in the **Value** box, and click Add; then select **Department (OU)** and type **Techpubs** in the **Value** box. Figure 4-2 shows what you have entered in the **Edit DN** dialog box.

Figure 4-2 Subject Name Attributes and Values



Step 4 After reviewing the dialog box, click **OK**, then click **OK** in the remaining two dialog boxes.

Obtaining Certificates with SCEP

The following sections show how to configure certificates using SCEP. Repeat the instructions for each trustpoint you configure for automatic enrollment. As you complete the instructions for each trustpoint, the ASA receives a CA certificate for the trustpoint and one or two certificates for signing and encryption purposes. If you do not follow these procedures, the ASA prompts you to paste the base-64 formatted CA certificate into the text box.

If you use DSA keys, the certificate received is for signing only.

If you use general-purpose RSA keys, the certificate received is for signing and encryption. If you use separate RSA keys for signing and encryption, the security appliance receives separate certificates for each purpose.

Using CLI Commands

Use the **crypto ca authenticate** command in global configuration mode to obtain certificates. Optionally, you can supply a fingerprint consisting of alphanumeric characters for the ASA to use to authenticate the CA certificate. Issuing this command puts you in interactive mode. The ASA displays the fingerprint of the certificate and prompts you to accept this certificate. To accept the certificate, type **yes** (or **y**).

Note This example shows how to confirm a certificate with a "fingerprint." However, not all CAs require this confirmation.

```
hostname(config)# crypto ca authenticate newmsroot
INFO: Certificate has the following attributes:
Fingerprint:     3736ffc2 243ecf05 0c40f2fa 26820675

Do you accept this certificate? [yes/no]: y

Trustpoint 'newmsroot' is a subordinate CA and holds a non self signed cert.
Trustpoint CA certificate accepted.
```

Using ASDM

To use ASDM to obtain certificates, follow these steps:

Step 1 Go to the **Configuration > Features > Device Administration > Certificate > Authentication** panel.

Step 2 In the **Trustpoint Name** list, select the name of the trustpoint. For this example, select **newmsroot**.

Step 3 Click **Authenticate**.

Step 4 Click **Apply**. When ASDM displays the **Authentication Successful** dialog, click **OK**.

Enrolling with the Certificate Authority

After you configure the trustpoint and authenticate with it, you can enroll for an identity certificate.

Using CLI Commands

You can use the **show running-config crypto ca certificates** *trustpoint_name* and **show running-config crypto ca trustpoint** *trustpoint_name* command to display the running configuration for a particular trustpoint.

When the trustpoint is configured for SCEP enrollment, as shown in the following example, the ASA displays a CLI prompt and displays status messages to the console.

To begin enrollment, use the **crypto ca enroll** command. The syntax is **crypto ca enroll** *trustpoint* [**noconfirm**]. Decide on a password before you start.

Note The interactive prompts vary depending on the configured state of the referenced trustpoint.

```
hostname(config)# crypto ca enroll newmsroot
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.

Password: v$bx8*c

Re-enter password: v$bx8*c
% The subject name in the certificate will be: CN=Pat, OU=Techpubs
% The fully-qualified domain name in the certificate will be: hostname.ciscopix.com

% Include the router serial number in the subject name? [yes/no]: y
% The serial number in the certificate will be: P3000000098

Request certificate from CA? [yes/no]: y
% Certificate request sent to Certificate Authority
hostname(config)# The certificate has been granted by CA!
```

You now have both the CA and the identity certificate.

Using ASDM

To enroll for an identity certificate using ASDM, follow these steps:

Step 1 Go to the **Configuration > Features > Device Administration > Certificate > Enrollment** panel.

Step 2 Select the trustpoint in the **Trustpoint Name** list. For this example, you would select **newmsroot**.

Step 3 Click **Enroll**.

Managing Certificates in ASDM

To manage certificates, go to the **Configuration > Features > Device Administration > Certificate > Manage Certificates** panel.

You can use this panel to add a new certificate and delete a certificate. You can also display information about a certificate by clicking **Show Details**. The Certificate Details dialog displays three tables: General, Subject and Issuer.

The **General** panel displays the following information:

- Type—CA, RA, or Identity
- Serial number—Serial number of the certificate
- Status—Available or pending
  - Available means that the CA has accepted the enrollment request and has issued an identity certificate.
  - Pending means that the enrollment request is still in process and that the CA has not issued the identity certificate yet.
- Usage—General purpose or Signature
- CRL distribution point (CDP)—URL for obtaining the CRL for validating the certificate
- Dates/times within which the certificate is valid—Valid from, valid to

The **Subject** table displays the following information:

- Name—The name of the person or entity that owns the certificate
- Serial number—The serial number of the ASA
- Distinguished (X.500) name fields for the subject of the certificate—cn, ou, etc.
- Hostname of the certificate holder

The **Issuer** table displays the distinguished name fields for the entity that granted the certificate.

- Common name (cn)
- Organizational unit or department (ou)
- Organization (o)
- Locality (l)
- State (st)
- Country code (c)
- Email address of the issuer (ea)

Configuring a LAN-to-LAN Tunnel

The easiest way to configure an IPSec LAN-to-LAN tunnel between the ASA and a peer device is to use the VPN wizard. For information on using the wizard, see "Configuring a VPN Tunnel Using the VPN Wizard" which contains a list of the information to gather before running the wizard.

Use this section if you want to configure a tunnel without using the wizard, or make changes after the initial configuration. This section shows how to configure a LAN-to-LAN tunnel using the CLI as well as ASDM. Also, this section explains some of the VPN terminology used by the ASA that is different from that used by the VPN 3000 Concentrator.

Building a LAN-to-LAN VPN connection includes the following tasks:

- Configuring Interfaces
- Configuring ISAKMP Policy and Enabling ISAKMP on the Outside Interface
- Creating a Transform Set
- Configuring an ACL
- Defining a Tunnel Group
- Creating a Crypto Map and Applying it to an Interface
- Permitting IPSec Traffic

Example Configuration

The commands shown below show how to configure a LAN-to-LAN connection. Later sections provide step-by-step instructions that explain how to configure this connection, and how to authenticate with preshared keys and certificates.

```
hostname(config)# interface ethernet0
hostname(config-if)# ip address 10.10.4.100 255.255.0.0
hostname(config-if)# nameif outside
hostname(config-if)# no shutdown
hostname(config)# isakmp policy 1 authentication pre-share
hostname(config)# isakmp policy 1 encryption 3des
hostname(config)# isakmp policy 1 hash sha
hostname(config)# isakmp policy 1 group 2
hostname(config)# isakmp policy 1 lifetime 43200
```

Note You only need to issue the following command once; it is not necessary for each tunnel.

```
hostname(config)# isakmp enable outside
hostname(config)# crypto ipsec transform set FirstSet esp-3des esp-md5-hmac
hostname(config)# access-list 121_list extended permit ip 192.168.0.0 255.255.0.0
150.150.0.0 255.255.0.0
hostname(config)# tunnel-group 10.10.4.108 type ipsec_l2l
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-ipsec)# pre-shared-key xyzx
hostname(config)# crypto map abcmap 1 match address xyz
hostname(config)# crypto map abcmap 1 set peer 10.10.4.108
hostname(config)# crypto map abcmap 1 set transform-set FirstSet
```

Note You only need to issue the following two commands once unless you build a tunnel to a different interface.

```
hostname(config)# crypto map abcmap interface outside
hostname(config)# sysopt connection permit-ipsec
hostname(config)# write mem
```

Configuring Interfaces

An ASA has at least four interfaces, two of which are referred to here as outside and inside. Typically, the outside interface is connected to the public Internet, while the inside interface is connected to a private network and is protected from public access.

Configure and enable two interfaces on the ASA, and assign a name, IP address and subnet mask. Optionally, configure its security level, speed, and duplex operation on the security appliance (not shown in this example).

Using CLI Commands

To configure interfaces in CLI, use the following steps and the command syntax in the examples as a guide.

Step 1 In global configuration mode, enter the **interface** command and the default name of the interface to be configured (for instance, ethernet0). Doing so places your session in interface configuration mode. For example,

```
hostname(config)# interface ethernet0
hostname(config-if)#
```

Step 2 Enter the **ip address** command and the IP address and subnet mask of the interface. In the following example, the IP address is 10.10.4.100 and the subnet mask is 255.255.0.0:

```
hostname(config-if)# ip address 10.10.4.100 255.255.0.0
hostname(config-if)#
```

Step 3 To name the interface, use the **nameif** command, maximum of 48 characters. You cannot change this name after you set it. In this example, the name of the ethernet0 interface is outside.

```
hostname(config-if)# nameif outside
hostname(config-if)#
```

Step 4 To enable the interface, use the **no** version of the **shutdown** command. By default, interfaces are disabled.

```
hostname(config-if)# no shutdown
hostname(config-if)#
```

Step 5 To save your changes, use the **write memory** command.

```
hostname(config-if)# write memory
hostname(config-if)#
```

Step 6 To configure a second interface, use the same procedure.

Using ASDM

To display the CLI commands that ASDM sends to the device, click the **Options** menu, click **Preferences**, and select **Preview commands before sending to the device**.

To configure these interfaces in the example using ASDM, follow these steps:

Step 1 Under the **Configuration > Features > Interfaces** panel, click **Add**. ASDM opens the **Add Interface** dialog box.

Step 2 Click an interface in the **Hardware Port** list. For this example, select **ethernet0**.

Step 3 Click **Enable Interface**.

Step 4 Type the name in the **Interface Name** box. For this example, the name is outside.

Step 5 Type the IP address in the **IP Address** box. For this example, the IP address is 10.10.4.100.

Step 6 Click a subnet mask in the **Subnet Mask** list. For this example, click **255.0.0.0**.

Step 7 Click the **Use Static IP** (for this example) and the click **OK**.

Step 8 To save the configuration, which you should do periodically, click **Save** on the tool bar and click **Yes**.

Configuring ISAKMP Policy and Enabling ISAKMP on the Outside Interface

Internet Security Association and Key Management Protocol (ISAKMP), also called IKE, is the negotiation protocol that lets two hosts agree on how to build an IPSec Security Association. Each ISAKMP negotiation is divided into two sections called Phase1 and Phase2.

Phase 1 creates the first tunnel, which protects later ISAKMP negotiation messages. Phase 2 creates the tunnel that protects data.

To set the terms of the ISAKMP negotiations, you create an ISAKMP policy, which includes the following:

- Authentication method to ensure the identity of the peers (either preshared key or certificate).
- Encryption method to protect the data and ensure privacy.
- Hashed message authentication codes (HMAC) method to ensure the integrity of the messages and the identity of the sender.
- Diffie-Hellman group to establish the strength of the algorithm that determines the encryption key. The ASA uses this algorithm to derive the encryption and hash keys.
- Expiration timer for the encryption key that determines when the ASA replaces it.

Table 4-1 provides information about the IKE policy keywords and their values.

Table 4-1 Phase 1 — IKE Policy Keywords for CLI Commands

Command	Keyword	Meaning	Description
isakmp policy authentication	rsa-sig dsa-sig pre-share	A digital certificate with keys generated by the RSA signatures algorithm A digital certificate with keys generated by the DSA signatures algorithm pre-shared keys	Specifies the authentication method the ASA uses to establish the identity of each IPSec peer.
isakmp policy encryption	des 3des aes aes-192 aes-256	56-bit DES-CBC 168-bit Triple DES	Specifies the symmetric encryption algorithm that protects data transmitted between two IPSec peers. The default is 56-bit DES-CBC, which is less secure and faster than the alternatives. The Advanced Encryption Standard supports key lengths of 128, 192, and 256 bits.
isakmp policy hash	sha md5	SHA-1 (HMAC variant) MD5 (HMAC variant)	Specifies the hash algorithm used to ensure data integrity. It ensures that a packet comes from whom you think it comes from and that it has not been modified in transit. The default is SHA-1. MD5 has a smaller digest and is considered to be slightly faster than SHA-1.
isakmp policy group	1 2 5 7	Group 1 (768-bit) Group 2 (1024-bit) Group 5 (1536-bit) Group 7 (Elliptical curve field size is 163 bits.)	Specifies the Diffie-Hellman group identifier, which the two IPSec peers use to derive a shared secret without transmitting it to each other. The default is Group 2 (1024-bit Diffie-Hellman).
isakmp policy lifetime	integer value	120 to 2147483647 seconds	Specifies the SA lifetime. The default is 86400 seconds or 24 hours. As a general rule, a shorter lifetime (up to a point) provides more secure IKE negotiations. However, with longer lifetimes, the ASA sets up future IPSec security associations more quickly.

Using CLI Commands

You can enter the **show run isakmp** command to display the current, operational isakmp configuration. The *priority* displayed after "policy" in the system response and in the commands that follow uniquely identifies the associated IKE policy and represents the priority assigned to the policy. It may be an integer from 1 to 65,534 with 1 being the highest priority and 65,534 the lowest.

To configure ISAKMP policies, in global configuration mode, use the **isakmp policy** command with its various arguments. The syntax for ISAKMP policy commands is:

isakmp policy *priority* **attribute_name** [**attribute_value** | *integer*]

Use the following steps and the command syntax in the examples as a guide.

Step 1 Set the authentication method. This example specifies RSA signatures as the authentication method. The default setting is **pre-share**. The priority is 1 in this step and the ones that follow.

```
hostname(config)# isakmp policy 1 authentication rsa-sig
hostname(config)#
```

Step 2 Set the encryption method. This example shows the default setting (**3des**).

```
hostname(config)# isakmp policy 1 encryption 3des
hostname(config)#
```

Step 3 Set the HMAC method. This example shows the default setting (**sha**).

```
hostname(config)# isakmp policy 1 hash sha
hostname(config)#
```

Step 4 Set the Diffie-Hellman group. This example configures Group 2.

```
hostname(config)# isakmp policy 1 group 2
hostname(config)#
```

Step 5 Set the encryption key lifetime. This example configures 43,200 seconds (12 hours). The default setting is **86400**.

```
hostname(config)# isakmp policy 1 lifetime 43200
hostname(config)#
```

Step 6 Enable ISAKMP on the interface named outside. (This attribute does not have a default setting.)

```
hostname(config)# isakmp enable outside
hostname(config)#
```

Step 7 Use the **write mem** command to save your changes.

```
hostname(config)# write mem
hostname(config)#
```

Using ASDM

To configure ISAKMP policy in ASDM, follow these steps:

Step 1 Under the **Configuration > Features > VPN > IKE > Policies** panel, click **Add**.

Step 2 Enter information from the example configuration:

a. Type **1** in the **Priority** box.

b. For a preshared key, click **pre-share** in the **Authentication** list. For certificate authentication, click **rsa-sig** instead.

c. Click **3des** in the **Encryption** list.

d. Click **sha** in the **Hash** list.

e. Click **2** in the **D-H group** list.

f. Type 43200 in the **Lifetime** box and click **Seconds** in the **Lifetime** list.

Step 3 Then to enable ISAKMP on the interface, in the **Configuration > Features > VPN > IKE > Global Parameters** panel, click the interface in the **Enable IKE** group box, and click **Enable**.

Creating a Transform Set

A transform set combines an encryption method and an authentication method. During the IPSec security association negotiation with ISAKMP, the peers agree to use a specific transform set to protect a specific data flow. The transform set must be the same for both peers.

You can create multiple transform sets, and then specify one or more of these transform sets in a crypto map entry. The ASA uses the transform set to protect the data flows for that crypto map entry access list.

The valid encryption methods are as follows:

- esp-des
- esp-3des
- esp-aes (128-bit encryption)
- esp-aes-192
- esp-aes-256
- esp-null

The valid authentication methods are as follows:

- esp-md5-hmac
- esp-sha-hmac

IPSec works in tunnel mode, which is the way in which IPSec is implemented between two ASAs that are connected over an untrusted network, such as the public Internet. This requires no configuration.

Using CLI Commands

You can enter the **show run cryptic ipsec** command to display the current, operational transform set configuration.

To configure a transform set via the CLI, in global configuration mode, use the **crypto ipsec transform-set** command. The syntax is:

crypto ipsec transform-set *transform-set-name encryption-method authentication-method*

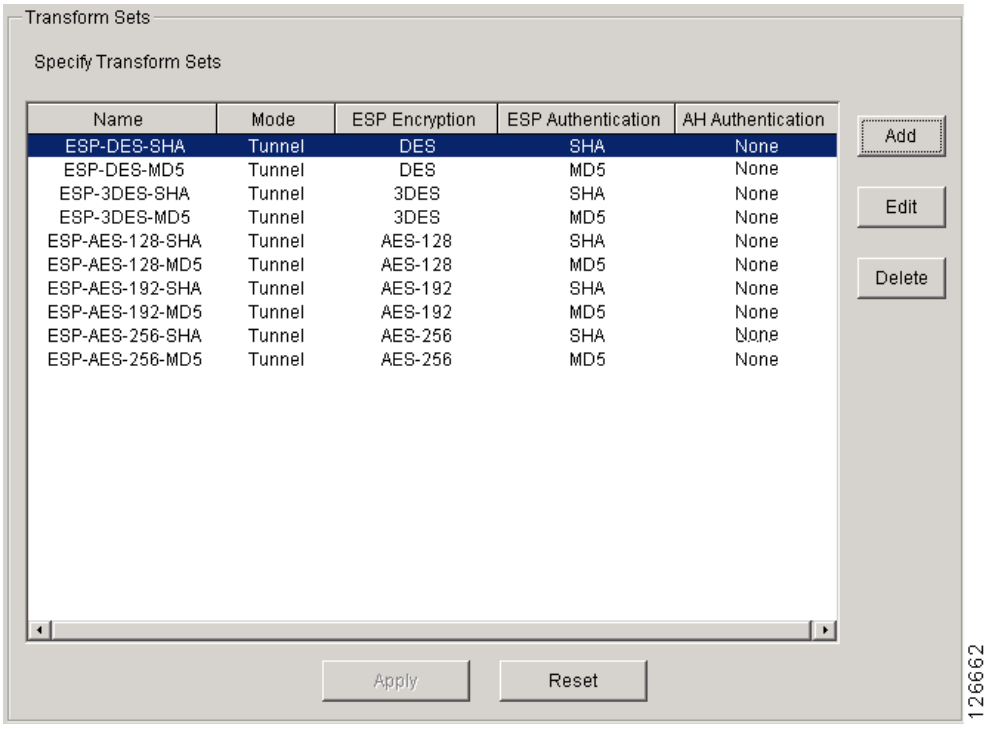
This example configures a transform set with the name FirstSet, esp-3des encryption, and esp-md5-hmac authentication.

```
hostname(config)# crypto ipsec transform-set FirstSet esp-3des esp-md5-hmac
hostname(config)#
```

Using ASDM

ASDM comes with all the standard transform sets already configured; most of the time there is no need to add one to the list. To view these transform sets, go to the **Configuration > Features > VPN > IPSec > Transform Sets** panel.

Figure 4-3 Transform Sets Table



Configuring an ACL

The ASA uses access control lists (ACLs) to control network access. By default, the ASA denies all traffic. You need to configure an ACL that permits traffic.

The ACLs you configure for a LAN-to-LAN VPN control connections based on source and destination IP addresses. Configure ACLs that mirror each other on both sides of the connection.

Using CLI Commands

Step 1 To configure an ACL, use the **access-list extended** command. The following example creates an ACL named l2l_list that lets traffic from IP addresses in the 192.168.0.0 network travel to the 150.150.0.0 network. The syntax is **access-list** *listname* **extended permit ip** *source-ipaddress source-netmask destination-ipaddress destination-netmask.*

```
hostname(config)# access-list l2l_list extended permit ip 192.168.0.0 255.255.0.0
150.150.0.0 255.255.0.0
hostname(config)#
```

Step 2 Configure an ACL for the ASA on the other side of the connection that mirrors the ACL above. For this example, the prompt for the peer is hostname2, and the command enables traffic to pass travel from the 150.150.0.0 network to the 192.168.0.0.

```
hostname2(config)# access-list l2l_list extended permit ip 150.150.0.0 255.255.0.0
192.168.0.0 255.255.0.0
hostname2(config)#
```

Using ASDM

To configure an ACL using ASDM, follow these steps:

Step 1 Under the **Configuration > Features > Security Policy > Access Rules** panel, click **Add**.

Step 2 For most of the fields, you can accept the defaults. You must enter the following information:

- IP address and mask for the source host/network (for example, this is 150.150.0.0/255.255.0.0)
- IP address and mask for the destination network (for example, this is 192.168.0.0/255.255.0.0)

Defining a Tunnel Group

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 ASA stores tunnel groups internally.

The two default tunnel groups in the ASA system are as follows:

- DefaultRAGroup, the default IPSec remote-access tunnel group.
- DefaultL2LGroup, the default IPSec LAN-to-LAN tunnel group.

You can modify these groups but you cannot delete them. You can also create one or more new tunnel groups to suit your environment. The ASA uses them to set 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; this example shows both a preshared key and certificate configuration.

Using CLI Commands

You can enter the **show run all tunnel** command to display the current, operational, tunnel group configuration.

Use the **tunnel-group** command to set the connection type to IPSec LAN-to-LAN, as follows:

Step 1 To set the connection type to IPSec LAN-to-LAN, use the **tunnel-group** command. The syntax is **tunnel-group** *name* **type** *type,* where *name* is the name you assign to the tunnel group, and *type* is the type of tunnel. The tunnel types as you enter them in the CLI are:

- ipsec_ra (IPSec remote access)
- ipsec_l2l (IPSec LAN to LAN)

In this example, the name of the tunnel group is the IP address of the LAN-to-LAN peer, 10.10.4.108.

```
hostname(config)# tunnel-group 10.10.4.108 type ipsec_l2l
hostname(config)#
```

Step 2 To set the authentication method, enter the ipsec-attributes mode and then use the **pre-shared-key** command to create the preshared key. You need to use the same preshared key on both ASAs for this LAN-to-LAN connection. For certificate authentication, use the **trust-point** command.

The preshared key is an alphanumeric string of 1-127 characters. In this example, the preshared key is xyzx. For certificate authentication, specify the trustpoint name, which in this example is newmsroot.

For preshared key authentication, the command is:

```
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-ipsec)# pre-shared-key xyzx
```

Or, for digital certificate authentication, the command is:

```
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-ipsec)# trust-point newmsroot
```

Using ASDM

To configure a tunnel group in ASDM using the information in this example:

Step 1 Under the **Configuration > Features > VPN > General > Tunnel Group** panel, click **Add**. ASDM displays the **Add Tunnel Group** dialog box, which resembles the User Management section in the VPN 3000 Concentrator Manager.

Step 2 In the **Identity** panel, type a name for the tunnel group in the **Name** box and click the **IPSec for LAN to LAN** option. The name can be the hostname or the IP address of the LAN-to-LAN peer (10.10.4.108 in this example).

Step 3 In the **IPSec** panel, for preshared key authentication, type the preshared key in the **Pre-shared Key** box. For this example, type **xyzx**. For certificate authentication, select the trustpoint name (**newmsroot**) in the **Trustpoint Name** list.

Creating a Crypto Map and Applying it to an Interface

Crypto map entries pull together the various elements of IPSec security associations, including the following:

- Which traffic IPSec should protect, which you define in an access list.
- Where to send IPSec-protected traffic, by identifying the peer.
- What IPSec security applies to this traffic, which a transform set specifies.
- The local address for IPSec traffic, which you identify by applying the crypto map to an interface.

For IPSec to succeed, both peers must have crypto map entries with compatible configurations. The entries may be IPSec Remote Access (ipsec-ra) or LAN-to-LAN (ipsec-l2l). For two crypto map entries to be compatible, they must, at a minimum, meet the following criteria:

- The crypto map entries must contain compatible crypto access lists (for example, mirror image access lists). If the responding peer uses dynamic crypto maps, the entries in the ASA crypto access list must be *permitted* by the peer's crypto access list.
- The crypto map entries each must identify the other peer (unless the responding peer is using a dynamic crypto map).
- The crypto map entries on each peer must have at least one transform set in common.

If you create more than one crypto map entry for a given interface, use the sequence number (seq-num) of each entry to rank it: the lower the sequence number, the higher the priority. At the interface that has the crypto map set, the ASA evaluates traffic against the entries of higher priority maps first.

Create multiple crypto map entries for a given interface if either of the following conditions exist:

- Different peers handle different data flows.
- You want to apply different IPSec security to different types of traffic (to the same or separate peers), for example, if you want traffic between one set of subnets to be authenticated, and traffic between another set of subnets to be both authenticated and encrypted. In this case, define the different types of traffic in two separate access lists, and create a separate crypto map entry for each crypto access list.

Using CLI Commands

You can enter the **show run crypto map** command to display the current, operational crypto map configuration.

To create a crypto map and apply it to the outside interface in global configuration mode, use several of the **crypto map** commands. These commands use a variety of arguments, but the syntax for all of them begins **crypto map** *map-name-seq-num*. In the examples for this command, the map-name is abcmap, and the sequence number is 1. Enter these commands in global configuration mode.

Step 1 To assign an access list to a crypto map entry, use the **crypto map match address** command.

The syntax is **crypto map** *map-name seq-num* **match address** *aclname*. In this example the map name is abcmap, the sequence number is 1, and the access list name is xyz.

```
hostname(config)# crypto map abcmap 1 match address xyz
hostname(config)#
```

Step 2 To identify the peer(s) for the IPSec connection, use the **crypto map set peer** command.

The syntax is **crypto map** *map-name seq-num* **set peer** {*ip_address1* | *hostname1*}[... *ip_address10* | *hostname10*]. In this example the hostname is 10.10.4.108.

```
hostname(config)# crypto map abcmap 1 set peer 10.10.4.108
hostname(config)#
```

Step 3 To specify a transform set for a crypto map entry, use the **crypto map set transform-set** command.

The syntax is **crypto map** *map-name seq-num* **set transform-set** *transform-set-name*. In this example the transform set name is FirstSet.

```
hostname(config)# crypto map abcmap 1 set transform-set FirstSet
hostname(config)#
```

Using ASDM

To configure crypto map functionality in ASDM, using information from the example configuration:

Step 1 Under the **Configuration > Features > VPN > IPSec > Tunnel Policy** panel, click **Add**.

Step 2 Select the interface and policy type:

a. Click **outside** in the **Interface** list.

b. Click **Static** in the **Policy Type** list.

Step 3 Type the priority (1) in the **Priority** box.

Step 4 Click a transform set from the **Transform Set to Be Added** list and click **Add**. For this example, click **ESP-3DES-MD5**.

Step 5 Select a connection type. For LAN to LAN, select **Bidirectional** in the **Connection Type** list.

Step 6 Enter the IP address of the peer device. If the connection type is bidirectional, you can enter only one peer device. Type the IP address (for this example, 192.168.1.1) in the **IP Address of Peer to be Added** box and click **Add**.

Applying Crypto Maps to Interfaces

When using the CLI interface, you must apply a crypto map set to each interface through which IPSec traffic travels. The ASA supports IPSec on all interfaces. Applying the crypto map set to an interface instructs the ASA to evaluate all interface traffic against the crypto map set and to use the specified policy during connection or security association negotiations. ASDM does this automatically.

Binding a crypto map to an interface also initializes the run-time data structures, such as the security association database and the security policy database. When you later modify a crypto map in any way, the ASA automatically applies the changes to the running configuration. It drops any existing connections and reestablishes them after applying the new crypto map.

To apply the configured crypto map to the outside interface, use the **crypto map interface** command.

The syntax is **crypto map** *map-name* **interface** *interface-name*

```
hostname(config)# crypto map abcmap interface outside
hostname(config)#
```

Permitting IPSec Traffic

The ASA accepts IPSec traffic only if you configure it to do so. The **sysopt** command permits IPSec traffic by letting tunneled traffic bypass interface ACLs to accept IPSec traffic. This means that decrypted traffic is not subject to interface ACLs.

Using CLI Commands

Using CLI commands, permit IPSec traffic and then save the configuration, as follows:

Step 1 Use the **sysopt** command in global configuration mode to have the ASA permit IPSec traffic.

```
hostname(config)# sysopt connection permit-ipsec
hostname(config)#
```

Step 2 Save your changes.

```
hostname(config)# write mem
hostname(config)#
```

Using ASDM

In ASDM, enable IPSec traffic and then save the configuration, as follows:

Step 1 Go to the **Configuration > Features > VPN > General > VPN System Options** panel.

Step 2 Click the **Enable IPSec authenticated inbound sessions to always be permitted through the ASA (that is, without a check of the access-list statements)** option.

Step 3 To save the running configuration to flash memory, click **Save** on the tool bar and then click **Yes** when ASDM asks you to confirm.

Configuring a Remote Access Tunnel

Building a remote access VPN tunnel includes the following tasks:

- Configuring Interfaces
- Configuring ISAKMP Policy and Enabling ISAKMP on the Outside Interface
- Configuring an Address Pool
- Adding a User
- Creating a Transform Set
- Defining a Tunnel Group
- Creating a Dynamic Crypto Map
- Creating a Crypto Map Entry to Use the Dynamic Crypto Map (CLI Only)
- Permitting IPSec Traffic

Example Configuration Overview

This document uses the following configuration to explain how to configure a remote access connection. Later sections provide step-by-step instructions. The instructions show how to authenticate with preshared keys and certificates.

```
hostname(config)# interface ethernet0
hostname(config-if)# ip address 10.10.4.200 255.255.0.0
hostname(config-if)# nameif outside
hostname(config-if)# # no shutdown
hostname(config)# isakmp policy 1 authentication pre-share
hostname(config)# isakmp policy 1 encryption 3des
hostname(config)# isakmp policy 1 hash sha
hostname(config)# isakmp policy 1 group 2
hostname(config)# isakmp policy 1 lifetime 43200
hostname(config)# isakmp enable outside
hostname(config)# ip local pool testpool 192.168.0.10-192.168.0.15
hostname(config)# username testuser password 12345678
hostname(config)# crypto ipsec transform set FirstSet esp-3des esp-md5-hmac
hostname(config)# tunnel-group testgroup type ipsec_ra
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-general)# address-pool testpool
hostname(config)# tunnel-group testgroup ipsec-attributes
hostname(config-ipsec)# pre-shared-key xyzx
hostname(config)# crypto dynamic-map dyn1 1 set transform-set FirstSet
hostname(config)# crypto dynamic-map dyn1 1 set reverse-route
hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1
hostname(config)# crypto map mymap interface outside
hostname(config)# sysopt connection permit-ipsec
hostname(config)# write mem
```

Configuring Interfaces

A security appliance has at least two interfaces, referred to here as outside and inside. Typically, the outside interface is connected to the public Internet, while the inside interface is connected to a private network and is protected from public access.

To begin, configure and enable two interfaces on the ASA. Then assign a name, IP address and subnet mask. Optionally, configure its security level, speed and duplex operation on the security appliance.

Using CLI Commands

To configure interfaces, follow these steps and use the command syntax in the examples.

Note To display the configuration of all interfaces, enter the **show interface** command.

Step 1 To enter Interface configuration mode, in global configuration mode use the **interface** command with the default name of the interface to configure. In this example the interface is ethernet0.

```
hostname(config)# interface ethernet0
hostname(config-if)#
```

Step 2 To set the IP address and subnet mask for the interface, use the **ip address** command. In this example the IP address is 10.10.4.200 and the subnet mask is 255.255.0.0.

```
hostname(config-if)# ip address 10.10.4.200 255.255.0.0
hostname(config-if)#
```

Step 3 To name the interface, use the **nameif** command, maximum of 48 characters. You cannot change this name after you set it. In this example, the name of the ethernet0 interface is outside.

```
hostname(config-if)# nameif outside
hostname(config-if)#
```


Note When you name the interface "outside," the ASA assigns the default settings ethernet0 and Security Level 0. When you name the interface "inside," the ASA assigns the default settings ethernet1 and Security Level 100.

Step 4 To enable the interface, use the **no** version of the **shutdown** command. By default, interfaces are disabled.

```
hostname(config-if)# no shutdown
hostname(config-if)#
```

Step 5 To save your changes, use the **write memory** command.

```
hostname(config-if)# write memory
```

Step 6 Using the same procedure, configure a second interface.

Using ASDM

To configure these interfaces in the example using ASDM, follow these steps:

Step 1 Under the **Configuration > Features > Interfaces** panel, click **Add**. ASDM opens the **Add Interface** dialog box.

Step 2 Click an interface in the **Hardware Port** list. For this example, select **ethernet0**.

Step 3 Click **Enable Interface**.

Step 4 Type the name in the **Interface Name** box. For this example, the name is outside.

Step 5 Type the IP address in the **IP Address** box. For this example, the IP address is 10.10.4.200.

Step 6 Click a subnet mask in the **Subnet Mask** list. For this example, the subnet mask is 255.0.0.0.

Step 7 Click the **Use Static IP** (for this example) and click **OK**.

Step 8 To save the configuration, which you should do periodically, click **Save** on the tool bar and click **Yes**.

Configuring ISAKMP Policy and Enabling ISAKMP on the Outside Interface

Internet Security Association and Key Management Protocol (ISAKMP) is the negotiation protocol that lets two hosts agree on how to build an IPSec Security Association. Each ISAKMP negotiation is divided into two sections called Phase1 and Phase2.

Phase 1 creates the first tunnel to protect later ISAKMP negotiation messages. Phase 2 creates the tunnel that protects data.

To set the terms of the ISAKMP negotiations, you create an ISAKMP policy. It includes the following:

- Authentication method to ensure the identity of the peers.

  This section shows both preshared key and certificate configurations.
- Encryption method to protect the data and ensure privacy.
- Hashed Message Authentication Codes (HMAC) method to ensure the identity of the sender and to ensure that the message has not been modified in transit.
- Diffie-Hellman group to set the size of the encryption key. The security appliance uses this algorithm to derive the encryption and hash keys.
- Encryption key expiration timer.

For more overview information, see Table 4-1 in the LAN-to-LAN section of this chapter.

Using CLI Commands

To configure ISAKMP policies, in global configuration mode, use the **isakmp policy** command with its various arguments. The syntax for ISAKMP policy commands is:

isakmp policy *priority* **attribute_name** [**attribute_value |** *integer*].

Use the following steps and the command syntax in the examples as a guide.

Step 1 Set the authentication method. The default setting is pre-share. The other options are **dsa-sig** and **rsa-sig** to use DSA or RSA signatures as the authentication method.

For example,

```
hostname(config)# isakmp policy 1 authentication pre-share
hostname(config)#
```

Step 2 Set the encryption method. This example configures 3DES.

```
hostname(config)# isakmp policy 1 encryption 3des
hostname(config)#
```

Step 3 Set the HMAC method. This example configures SHA.

```
hostname(config)# isakmp policy 1 hash sha
hostname(config)#
```

Step 4 Set the Diffie-Hellman group. This example configures Group 2.

```
hostname(config)# isakmp policy 1 group 2
hostname(config)#
```

Step 5 Set the encryption key lifetime. This example configures 43, 200 seconds (12 hours).

```
hostname(config)# isakmp policy 1 lifetime 43200
hostname(config)#
```

Step 6 Enable ISAKMP on the interface named outside.

```
hostname(config)# isakmp enable outside
hostname(config)#
```

Step 7 Use the **write mem** command to save your changes.

```
hostname(config)# write mem
hostname(config)#
```

Using ASDM

To configure ISAKMP policy in ASDM, follow these steps:

Step 1 Under the **Configuration > Features > VPN > IKE > Policies** panel, click **Add**.

Step 2 Enter information from the example configuration:

a. Type **1** in the **Priority** box.

b. For preshared key, click **pre-share** in the **Authentication** list. For certificate authentication, click **rsa-sig** instead.

c. Click **3des** in the **Encryption** list.

d. Click **md5** in the **Hash** list.

e. Click **2** on the **D-H group** list.

f. Type 43200 in the **Lifetime** box and click **Seconds** on the **Lifetime** list.

Step 3 To enable ISAKMP on the interface, go to the **Configuration > Features > VPN > IKE > Global Parameters** panel, click the interface in the **Enable IKE** box, and click **Enable**.

Configuring an Address Pool

Asecurity appliance requires a method for assigning IP addresses to users. A common method is using address pools. The alternatives are having a DHCP server assign addresses or having an AAA server assign them. This example uses an address pool.

Using CLI Commands

When configuring an address pool, you must supply the mask value if the IP addresses assigned to VPN clients belong to a non-standard network, and the data could be routed incorrectly if you use the default mask. A typical example is when the IP local pool contains 10.10.10.0/255.255.255.0 addresses, since this is a Class A network by default. This could cause some routing issues when the VPN client needs to access different subnets within the 10 network over different interfaces. For example, if a printer, address 10.10.100.1/255.255.255.0 is available via interface 2, but the 10.10.10.0 network is available over the VPN tunnel and therefore interface 1, the VPN client would be confused as to where to route data destined for the printer. Both the 10.10.10.0 and 10.10.100.0 subnets are in the 10.0.0.0 Class A network so the printer data may be sent over the VPN tunnel.

To configure an address pool, use the **ip local pool** command. The syntax is **ip local pool** *poolname first_address-last_address* [**mask** *mask*]. The following example command configures an IP address pool named firstpool. The starting address is 10.20.30.40 and the ending address is 10.20.30.50. The network mask is 255.255.255.0.

```
hostname(config)# ip local pool firstpool 10.20.30.40-10.20.30.50 mask 255.255.255.0
hostname(config)#
```

Use the **show running-config ip local pool** command to display the address pool configuration.

Using ASDM

To configure an address pool in ASDM, follow these steps:

Step 1 Under the **Configuration > Features > VPN > IP Address Management > IP Pools** panel, click **Add**.

Step 2 Enter the name, starting IP address, and ending IP address. For this example:

a. Type testpool in the **Name** box.

b. Type **192.168.0.10** in the **Start IP** box.

c. Type **192.168.0.15** in the **End IP** box.

Step 3 In the **Subnet Mask** list, click one of the standard network masks, for this example, click **255.255.255.0**.

Adding a User

To identify remote access users to the ASA, configure usernames and passwords.

Using CLI Commands

To configure an entry in the internal database for each user, use the **username** command. The syntax is **username** *username* **password** *password*. In this example the username is testuser and the password is 12345678. For information on setting up external authentication, see "Authenticating with External Servers."

```
hostname(config)# username testuser password 12345678
hostname(config)#
```

Using ASDM

To configure usernames and passwords in ASDM, follow these steps:

Step 1 Under the **Configuration > Features > Device Administration > Administration > User Accounts** panel, click **Add**.

Step 2 Enter the username and password, confirm password, and optionally a privilege level. For this example:

a. Under the **Identity** panel, type **testuser** in the **User Name** box.

b. Type **12345678** in the **Password** box.

c. Type the password again in the **Confirm Password** box.

Creating a Transform Set

A transform set combines an encryption method and an authentication method. During the IPSec security association negotiation with ISAKMP, the peers agree to use a specific transform set to protect a specific data flow. The transform set must be the same for both peers.

You can create multiple transform sets to support tunnel combinations comprising different attributes, and then specify one or more of these transform sets in a crypto map entry. The ASA uses the transform set to protect the data flows for that crypto map entry access list. For more overview information, including a table that lists valid encryption and authentication methods, see the LAN-to-LAN "Creating a Transform Set" section.

Using CLI Commands

To configure a transform set, in global configuration mode, use the **crypto ipsec transform-set** command. The syntax is:

crypto ipsec transform-set *transform-set-name encryption-method authentication-method*

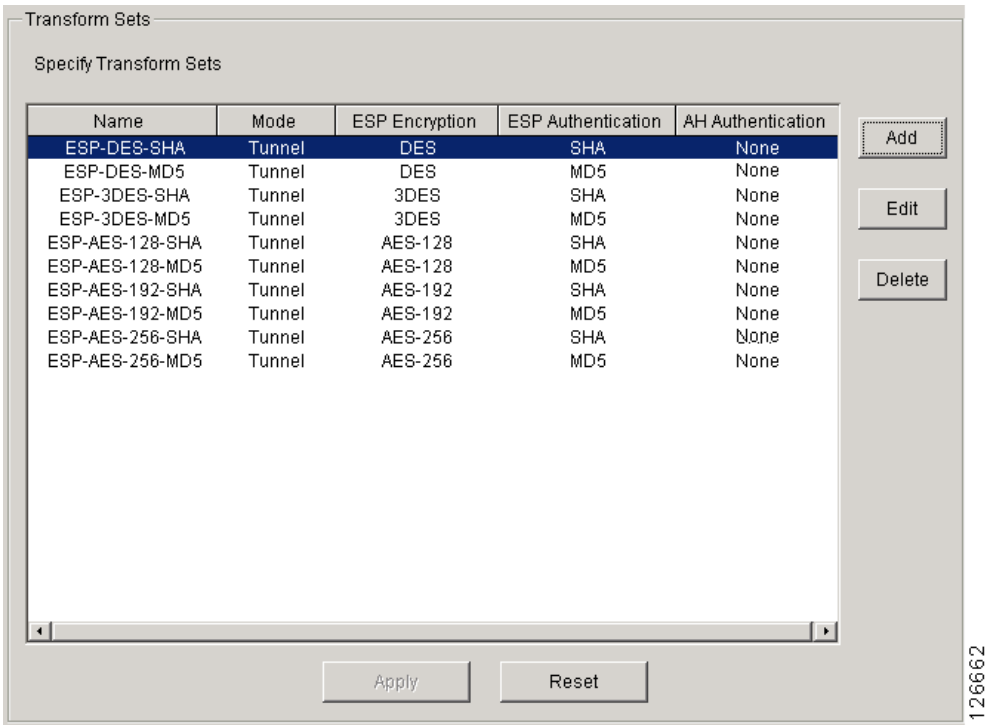
This example configures a transform set with the name FirstSet, esp-3des encryption, and esp-md5-hmac authentication.

```
hostname(config)# crypto ipsec transform set FirstSet esp-3des esp-md5-hmac
hostname(config)#
```

Using ASDM

ASDM comes with all the standard transform sets already configured; most of the time there is no need to add one to the list. To view these transform sets, go to the **Configuration > Features > VPN > IPSec > Transform Sets** panel.

Figure 4-4 Transform Sets Table



Defining a Tunnel Group

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 ASA stores tunnel groups internally.

Two default tunnel groups in the ASA system are: DefaultRAGroup, the default IPSec remote-access tunnel group; and DefaultL2Lgroup, the default IPSec LAN-to-LAN tunnel group. You can change them but not delete them. The ASA uses them 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 remote access connection, you must set three attributes for a tunnel group:

- Set the connection type to IPSec_RA (remote access).
- Configure the address assignment method. The following steps show an address pool.
- Configure an authentication method. The following steps show both a preshared key and a digital certificate.

Using CLI Commands

You can enter the **show run all tunnel** command to display the current, operational, tunnel group configuration.

Use the CLI to configure a trunk group, as follows:

Step 1 To set the connection type to IPSec remote access, use the **tunnel-group** command. The command syntax is **tunnel-group** *name* **type** *type,* where *name* is the name you assign to the tunnel group, and *type* is the type of tunnel. The tunnel types as you enter them in the CLI are:

- ipsec_ra (IPSec remote access)
- ipsec_l2l (IPSec LAN to LAN)

In this example, the name of the tunnel group is testgroup and the type is ipsec_ra.

```
hostname(config)# tunnel-group testgroup type ipsec_ra
hostname(config)#
```

Step 2 To configure an address pool for the tunnel group, enter the general-attributes mode and then use the **address-pool** command to create the address pool. In this example, the name of the group is testgroup and the name of the address pool is testpool.

```
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-general)# address-pool testpool
```

Step 3 To configure the authentication method, enter the ipsec-attributes mode and then use the **pre-shared-key** command to create the preshared key. You need to use the same preshared key on both devices for this remote-access connection. For certificate authentication, use the **trust-point** command.

The preshared key is an alphanumeric string of 1-127 characters. In this example, the preshared key is xyzx. For certificate authentication, you specify the trustpoint name, which in this example is newmsroot.

For preshared key authentication, the command is:

```
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-ipsec)# pre-shared-key xyzx
```

For digital certificate authentication, the command is:

```
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-ipsec)# trust-point newmsroot
```

Using ASDM

Use the ASDM to configure a trunk group, as follows:

Step 1 Go to the **Configuration > Features > VPN > General > Tunnel Group** panel and click **Add**.

Step 2 In the **Identity** panel, type the tunnel group name in the **Name** box; for this example the name is testgroup.

Step 3 In the **Type** group, click the **IPSec for Remote Access** option.

Step 4 In the **Client Address Assignment** panel, in the **Address Pool** group, select the address pool you added previously and click **Add**.

Step 5 In the **IPSec** panel, for preshared key, type the preshared key in the **Pre-shared Key** box. For this example, the preshared key is xyzx. Alternatively, for certificate authentication, select the name of the trustpoint in the **Trustpoint Name** list. For this example, the name is newmsroot.

Creating a Dynamic Crypto Map

The ASA uses dynamic crypto maps to define a policy template. These dynamic crypto maps let the ASA receive connections from peers without known IP addresses. Remote access clients are in this category.

Dynamic crypto map entries identify the transform set for the connection. You also enable reverse route injection (RRI), which lets the ASA learn routing information for connected clients. The ASA must also advertise it via RIP or OSPF. For clients that obtain their address from all methods (AAA, IP pools, and DHCP proxy), the ASA announces configured routes. For other address assignment methods, it uses a global enable/disable flag to determine the advertisement of client routes.

Using CLI Commands

You can enter the **show run all crypto dynamic-map** command to display the current, operational crypto dynamic map configuration.

To configure dynamic crypto map functionality in the CLI, using information from the example configuration, follow these steps:

Step 1 To specify a transform set for a dynamic crypto map entry, use following command syntax:

crypto dynamic -map *dynamic-map-name seq-num* **set transform-set** *transform-set-name*

In the following example, the name of the dynamic map is dyn1, the sequence number is 1, and the transform set name is FirstSet:

```
hostname(config)# crypto dynamic-map dyn1 1 set transform-set FirstSet
hostname(config)#
```

Step 2 To enable RRI for any connection based on this crypto map entry, use the **crypto dynamic-map set reverse route** command, as follows:

```
hostname(config)# crypto dynamic-map dyn1 1 set reverse-route
hostname(config)#
```

Step 3 Save your changes.

```
hostname(config)# write mem
hostname(config)#
```

Using ASDM

To configure dynamic crypto map functionality in ASDM, using information from the example configuration, follow these steps:

Step 1 Under the **Configuration > Features > VPN > IPSec > Tunnel Policy** panel, click **Add**.

Step 2 Click an interface in the **Interface** box. For this example, click **outside**.

Step 3 Click **dynamic** in the **Policy Type** box.

ASDM names the dynamic map by combining the interface and policy type. In this example, the name of the crypto dynamic map becomes outside_dyn_map.

Step 4 Type the priority (**1**) in the **Priority** box.

Step 5 Click a transform set in the **Transform Set to Be Added** list and click **Add**. For this example, click **ESP-3DES-MD5**.

Step 6 Click **Advanced**.

Step 7 Click the **Enable Reverse Route Injection** option.

Step 8 Click **OK** to exit the **Tunnel Policy Advanced Settings** dialog box and then click **OK** again to exit the **Add Tunnel Policy** dialog box.

Step 9 Click **Apply**.

Figure 4-5 shows the CLI commands generated by the tunnel policy configuration. Notice that ASDM has generated crypto map commands that reference the crypto dynamic map outside_dyn_map.

Figure 4-5 Tunnel Policy

```
crypto dynamic-map outside_dyn_map 1 set transform-set ESP-3DES-MD5
crypto dynamic-map outside_dyn_map 1 set security-association lifetime seconds 28800 kilobyte
crypto dynamic-map outside_dyn_map 1 set nat-t-disable
crypto dynamic-map outside_dyn_map 1 set reverse-route
crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
crypto map outside_map interface outside
```

Creating a Crypto Map Entry to Use the Dynamic Crypto Map (CLI Only)

If you are using the CLI, you must next create a crypto map entry that lets the ASA use the dynamic crypto map to set the parameters of IPSec security associations.

Note You do not have to create a crypto map to use the dynamic crypto map when you use ASDM. ASDM creates the crypto map automatically.

In the examples for this command, the name of the crypto map is mymap, the sequence number is 1, and the name of the dynamic crypto map is dyn1, the one created in the previous section Creating a Dynamic Crypto Map. Enter these commands in global configuration mode.

Step 1 To create a crypto map entry that uses a dynamic crypto map, use the **crypto map** command. The syntax is **crypto map** *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name.*

```
hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1
hostname(config)#
```

Step 2 To apply the crypto map to the outside interface, use the **crypto map interface** command.

The syntax is **crypto map** *map-name* **interface** *interface-name*

```
hostname(config)# crypto map mymap interface outside
hostname(config)#
```

Permitting IPSec Traffic

The ASA permits IPSec traffic only if you configure it to do so. The **sysopt** command permits IPSec traffic by letting tunneled traffic bypass interface ACLs to accept IPSec traffic. This means that decrypted traffic is not subject to interface ACLs.

Using CLI Commands

Using CLI commands, permit IPSec traffic and then save the configuration, as follows:

Step 1 Use the **sysopt** command in global configuration mode to have the ASA permit IPSec connections.

```
hostname(config)# sysopt connection permit-ipsec
hostname(config)#
```

Step 2 Save your changes.

```
hostname(config)# write mem
hostname(config)#
```

Using ASDM

In ASDM, permit IPSec traffic and then save the configuration, as follows:

Step 1 Click the **Configuration > Features > VPN > General > VPN System Options** panel.

Step 2 Click the **Enable IPSec authenticated inbound sessions to always be permitted through the ASA (that is, without a check of the access-list statements)** option.

Step 3 To save the running configuration to flash memory, click **Save** on the tool bar and then click **Yes** when ASDM asks you to confirm.

Performing Selected User Management Tasks

This chapter demonstrates how to configure several ASA user management features configurable in the User Management section of the VPN 3000 Concentrator Manager. In the ASA, you use group policies and tunnel groups to configure all of the features previously configurable as base group, group, and user attributes.

This chapter describes the following user management tasks:

Note ASDM comes with a complete online-help system. For field definitions on any panel, click **Help**.

For the complete syntax of the commands used in this chapter, see *Cisco Security Appliance Command Reference*.

Configuring Split Tunneling and Network Lists

Split tunneling lets an IPSec client conditionally direct packets over an IPSec tunnel in encrypted form, or to a network interface in cleartext form. Packets not bound for destinations on the other side of the IPSec tunnel do not have to be encrypted, sent across the tunnel, decrypted, and then routed to a final destination. Thus, split tunneling simplifies traffic management and eases the processing load.

Split tunneling applies only to single-user remote-access IPSec tunnels, not to LAN-to-LAN connections.

Split tunneling is primarily a traffic management feature, not a security feature. In fact, for optimum security, Cisco recommends that you *not* enable split tunneling. However, since only the security appliance—and not the IPSec client—can enable split tunneling, you can control implementation and thus protect security. Split tunneling is disabled by default on both the security appliance and the IPSec client. You enable and configure the feature on the ASA, and then the ASA uses ISAKMP to push it to, and enable it on, the IPSec client.

The example commands in this section show how to configure a network list using the access-list command in the CLI or the ACL Manager in ASDM. They also show how to set up an internal group policy for split tunneling that uses the network list and how to configure a remote-access tunnel group that uses the group policy.

Overview of Configuration Procedure

You configure split tunneling as follows:

1. Define a network list using standard access-lists.
2. Create a split tunneling group policy or modify the default remote access group policy.
3. Create a tunnel group for split tunneling.

The instructions in this section refer to the following scenario:

- The name of the network list is split.
- The name of the group policy is splitgroup.
- The name of the tunnel group is splittunnel.
- The tunnel group type is IPSec_RA.
- The tunnel group uses preshared keys for authentication.

For example,

```
hostname(config)# access-list split standard permit 172.16.1.0 255.255.255.0
hostname(config)# access-list split standard permit 192.168.1.0 255.255.255.0
hostname(config)# group-policy splitgroup internal
hostname(config)# group-policy splitgroup attributes
    hostname(config-group-policy)# split-tunnel-policy tunnelspecified
    hostname(config-group-policy)# split-tunnel-network-list value split
hostname(config)# tunnel-group splittunnel type ipsec_ra
hostname(config)# tunnel-group splittunnel general-attributes
    hostname(config-general)# default-group-policy splitgroup
hostname(config)# tunnel-group splittunnel ipsec-attributes
    hostname(config-ipsec)# pre-shared-key v$bx8*c
```

Defining a Network List

Start by defining a network list that permits secure traffic flow to specified networks at the central organization. For illustration, in the following sections, the network addresses are 172.16.1.0 255.255.255.0 and 192.168.1.0 255.255.255.0, and the identifier of the network list is split.

Using CLI Commands

To define the network list, use the access-list command. The syntax of the command in this example is:

access-list *identifier* **standard permit** *ipaddress*

Note The access list must be the standard type and not extended.

To permit traffic to these addresses, use the following **access-list** command:

```
hostname(config)# access-list split standard permit 172.16.1.0 255.255.255.0
hostname(config)# access-list split standard permit 192.168.1.0 255.255.255.0
```

Using ASDM

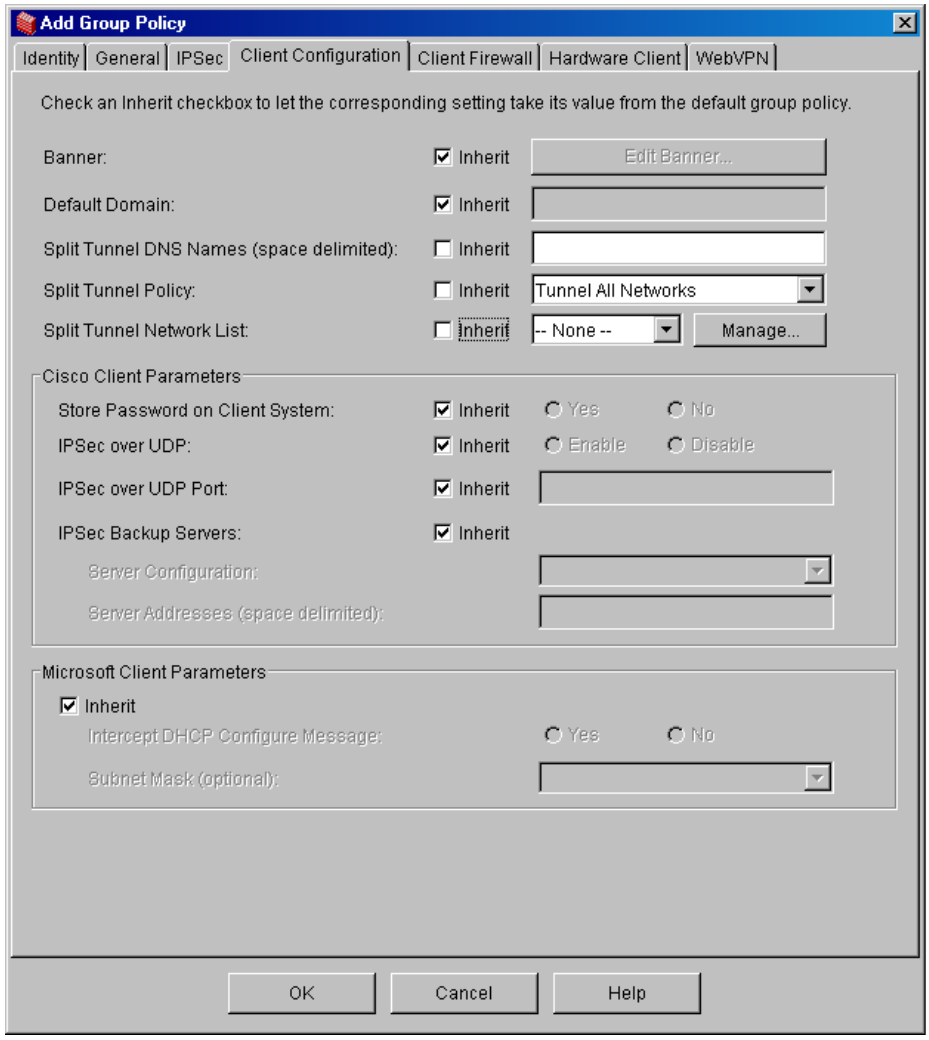
This section shows how to configure network lists for split tunneling using ASDM. In ASDM, you define network lists and other split tunneling parameters under the **Group Policy** panel.

To define network lists, use the ACL Manager, accessible from the **Group Policy Add/Edit Client Configuration** tab. Add a network list for split tunneling (or edit an existing group).

Step 1 Under the **Configuration > Features > VPN > General > Group Policy** panel, click **Add**. The **Group Policy Add** dialog box appears and displays the **Identity** tab.

Step 2 Click the **Client Configuration** tab. ASDM displays the **Client Configuration** options (see Figure 5-1).

Figure 5-1 Adding a Group Policy—Client Configuration



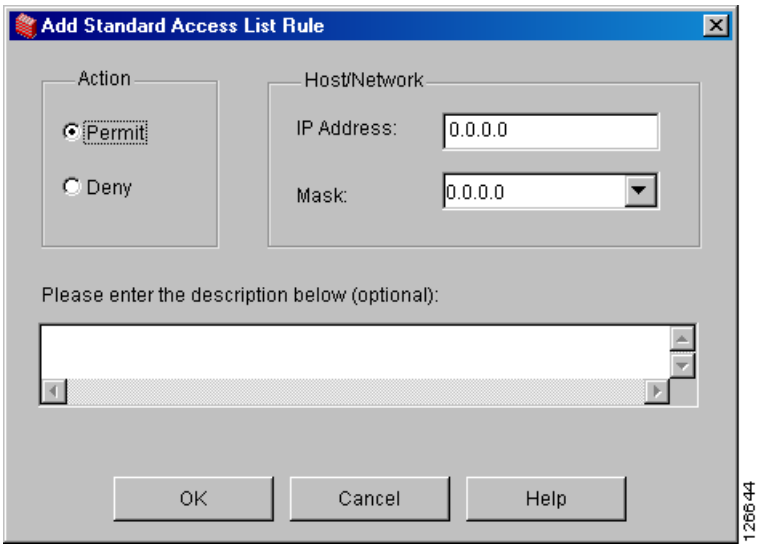
Step 3 To start defining a network list, click to uncheck the **Inherit** box next to **Split Tunnel Network List**.

Step 4 Click **Manage**. The **ACL Manager** table displays.

Step 5 To add an ACL, click **Add**. Type the ACL ID into the **ACL ID** box and click **OK**. In this example, the name is split.

Step 6 Click **Add ACE**. The **Add Standard Access List Rule** dialog box appears (see Figure 5-2).

Figure 5-2 Add an ACL for Split Tunneling



Step 7 Configure the options as follows:

- **Action** options—To include the network in the network list, click the **Permit** option.
- **Host/Network** group box—Configure the IP Address and subnet mask of each host or network to include for tunneling traffic securely to the corporate network.
  - **IP Address**—Type the IP Address in the text box. For this example, the IP address is 172.16.1.0.
  - **Mask**—Click on a subnet mask in the list. For this example, the subnet mask is 255.255.255.0.

Creating a Split Tunneling Group Policy

The following sections show how to create a split tunneling group policy or modify the default group policy (DfltGrpPolicy). The example configuration creates a specific group policy for split tunneling named splitgroup.

Using CLI Commands

Using **group-policy** commands, configure split tunneling policy in config-group-policy mode. The split-tunnel-policy attribute has the following options:

- **excludespecified**—Excludes only the specified networks. Sends all data via the secure IPSec tunnel except for data to addresses on the network list. In this case the ASA tunnels all traffic except to specified networks or hosts.
- **tunnelall**—Tunnels everything. This is the default split tunneling policy and disables split tunneling. When configured, all traffic from remote clients in the tunnel group travels over the secure IPSec tunnel in encrypted form.

- **tunnelspecified**—Tunnels only specified networks. Sends data to addresses on the network list via a secure IPSec tunnel. Data bound for any other address goes in the clear. This option lets remote users access internet networks without requiring them to be tunneled through the corporate network and lets them use specified resources on the corporate network through a secure tunnel.

The following example commands use the **tunnelspecified** option to tunnel traffic to the networks in the network list created in step 1.

```
hostname(config)# group-policy splitgroup internal
hostname(config)# group-policy splitgroup attributes
hostname(config-group-policy)# split-tunnel-policy tunnelspecified
hostname(config-group-policy)# split-tunnel-network-list value split
```

Using ASDM

Add a group policy for split tunneling, or edit an existing group, as follows:

Step 1 Under the **Configuration > Features > VPN > General > Group Policy** panel, click **Add**. ASDM displays the **Identity** tab.

Step 2 When adding a group policy, type a name in the **Name** box; for this example, the name is splitgroup. Click an option in the **Type** group box. For this example, click the **Internal** option. To select an external server such as RADIUS, you would click the **External** option, and enter the information for the server.

Step 3 To set up the split tunneling policy, click the **Client Configuration** tab. By default, the split tunneling parameters are disabled.

Step 4 Click to uncheck the **Inherit** box next to **Split Tunnel Policy** and click one of the following:

- **Tunnel All Networks**—This is the default split tunneling policy and disables split tunneling. When configured, all traffic from remote clients in the tunnel group travels over the secure IPSec tunnel in encrypted form. No traffic goes in the clear or to any destination other than the ASA. Remote users in the tunnel group reach internet networks through the corporate network and do not have access to local networks.
- **Tunnel Network List Below**—Sends data to addresses on the network list via a secure IPSec tunnel. Data bound for any other address goes in the clear. This option lets remote users access internet networks without requiring them to be tunneled through the corporate network and lets them use specified resources on the corporate network through a secure tunnel.
- **Exclude Network List Below**—Sends all data via the secure IPSec tunnel except for data to addresses on the network list. In this case, the ASA tunnels all traffic except to specified networks or hosts.

  The **Exclude Network List Below** option lets all users in the tunnel group access all devices on their local networks. If you want to restrict user access to specific devices on the local network, you need to know the addresses of the local devices the remote users in the tunnel group want to access. Create a network list of these addresses, then choose that network list from the Split Tunneling Network List. You can apply only one network list to a tunnel group, but one network list can contain up to 10 network entries. You also must enable **Local LAN Access** on the Cisco VPN client. See the *Cisco VPN Client Administrator Guide* for more details.

  For this example, click **Tunnel Network List Below**.

Configuring a Tunnel Group for Split Tunneling

Finally, use the instructions in one of the following sections to add a tunnel group for split tunneling, or edit an existing group. The examples in the instructions show how to add a remote-access tunnel group named splittunnel, and assign it a default group policy that provides split tunneling.

Using CLI Commands

Create a tunneling group for split tunneling as follows:

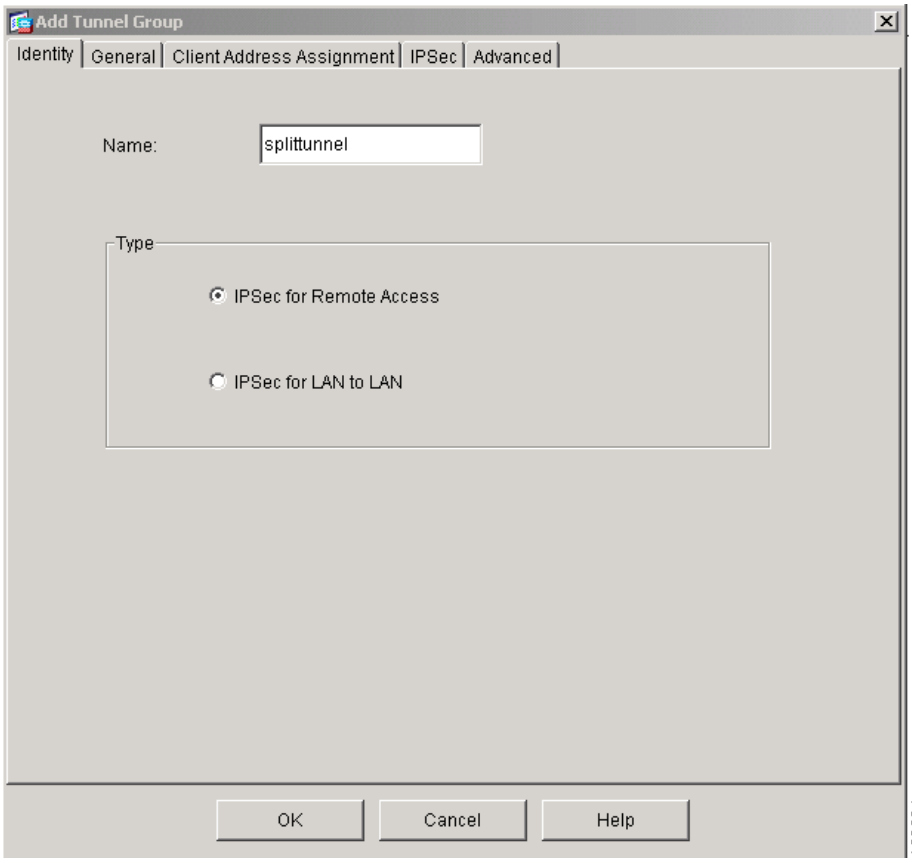
```
hostname(config)# tunnel-group splittunnel type ipsec_ra
hostname(config)# tunnel-group splittunnel general-attributes
hostname(config-general)# default-group-policy splitgroup
hostname(config)# tunnel-group splittunnel ipsec-attributes
hostname(config-ipsec)# pre-shared-key v$bx8*c
```

Using ASDM

Create a tunneling group for split tunneling as follows:

Step 1 Under the **Configuration > Features > VPN > General > Tunnel Group** panel, click **Add**. By default, the **Add Tunnel Group** dialog box displays the **Identity** tab (see Figure 5-3).

Figure 5-3 Adding a Tunnel Group—Identity tab



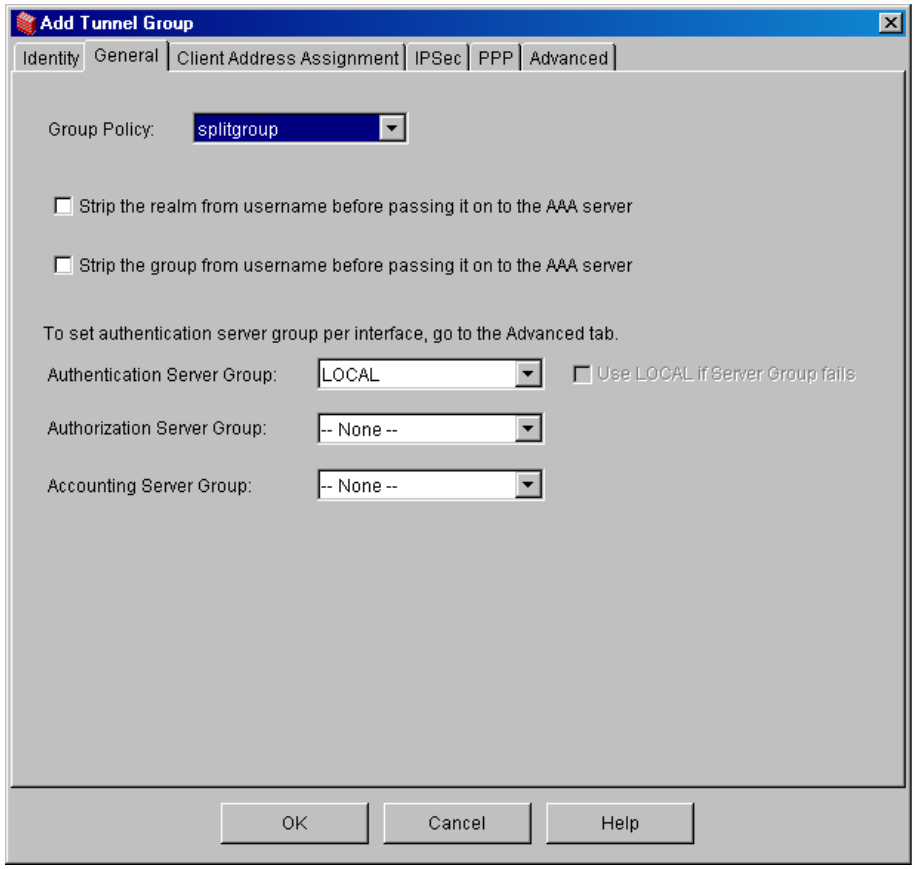
Step 2 Type the name for the tunnel group in the **Name** box.

For this example, the name is splittunnel.

Step 3 In the **Type** group box, click the **IPSec for Remote Access** option.

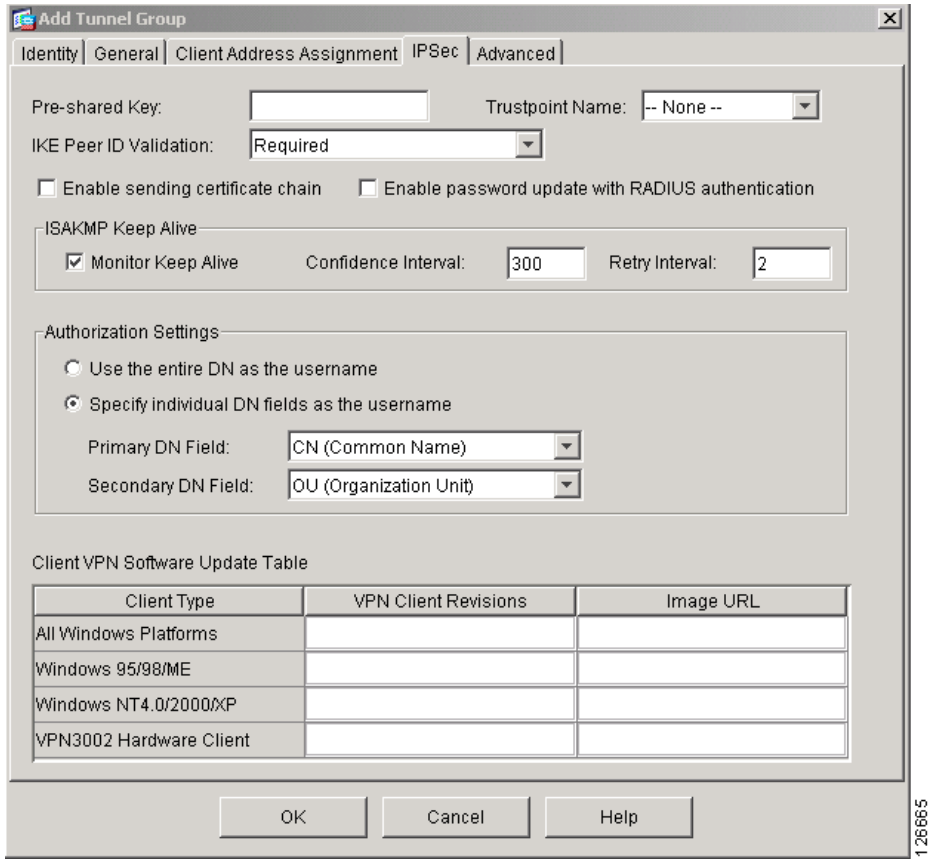
Step 4 Click the **General** tab and select the group policy from the **Group Policy** list. For this example, click **splitgroup**, the group policy configured in the previous section (see Figure 5-4).

Figure 5-4 Adding Tunnel Group—General tab



Step 5 Click the **IPSec** tab and type the preshared key in the **Pre-shared Key** box. For this example, type **cisco** and click **OK**. Then click **Apply** (see Figure 5-5).

Figure 5-5 Adding a Tunnel Group—IPSec Tab



Split DNS Names

Split DNS lets an internal DNS server resolve a list of centrally-defined *local domain names*, while ISP-assigned DNS servers resolve all other DNS requests. It is for split-tunneling connections; the internal DNS server resolves the domain names for traffic through the tunnel, and the ISP-assigned DNS servers resolve DNS requests that travel in the clear to the Internet.

The ASA does not support split-DNS for Microsoft VPN clients; however, it does support split DNS for the Cisco VPN client operating on Microsoft Windows operating systems.

Enter each domain name to be resolved by the internal server. Use only spaces to separate the names.

Configuring a Client Firewall and VPN

Note Only VPN clients running Microsoft Windows can use these firewall features. They are presently not available to hardware clients or other (non-Windows) software clients.

Client firewalls provide extra security if remote users in a tunnel group have split tunneling configured. In this case, the firewall protects the user's PC, and thereby the corporate network, from intrusions by way of the Internet or the user's local LAN.

Remote users connecting from the VPN client to the ASA can choose one of two firewall options.

In the first option, a remote user has a personal firewall installed on the PC. The VPN client enforces firewall policy defined on the local firewall, and it monitors that firewall to make sure it is running. If the firewall stops running, the VPN client drops the connection to the ASA. (This firewall enforcement mechanism is called *Are You There (AYT)*, because the VPN client monitors the firewall by sending it periodic "are you there?" messages; if no reply comes, the VPN client knows the firewall is down and terminates its connection to the security appliance.) The network administrator might configure these PC firewalls originally, but with this approach, users can customize their own configurations.

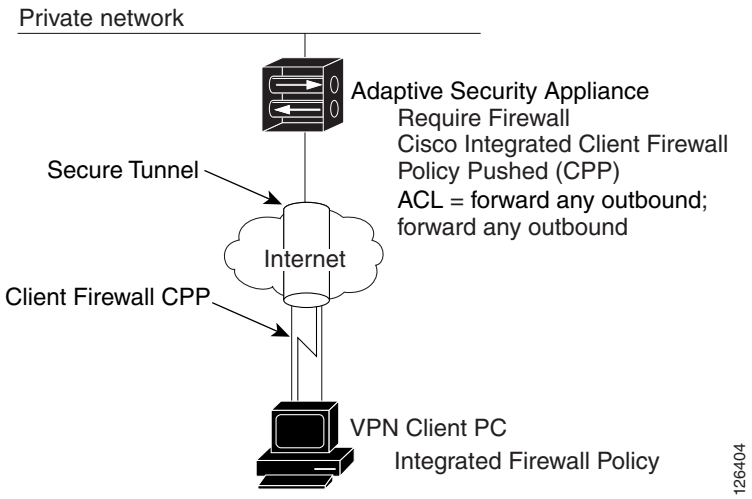
In the second option, you might prefer to enforce a centralized firewall policy for personal firewalls on VPN client PCs. A common example would be to block Internet traffic to remote PCs in a tunnel group using split tunneling. This approach protects the PCs, and therefore the central site, from intrusions from the Internet while tunnels are established. This firewall scenario is called *push policy* or *Central Protection Policy (CPP)*. On the ASA, you designate CPP as the firewall policy to enforce on the VPN client, and add ACLs for inbound and outbound traffic. The ASA then pushes this policy down to the VPN client. The VPN client passes the policy to the local Cisco Integrated Client firewall, which enforces it.

Configuring a Client Firewall to Use as a Default

The instructions in this section use the following scenario for illustration (see Figure 5-6):

- The firewall is required. Cisco Integrated Client firewall is the firewall type.
- Two access lists that can be used as defaults in a split tunneling configuration. The first denies all unsolicited traffic coming inbound to VPN clients from the Internet (or other sites outside the tunnel). This ACL is called FWBlockIn. The second permits outbound traffic from VPN clients to sites outside the tunnel. This ACL is called FWAllowAnyOut. The protocol for both is IP.

Figure 5-6 Cisco Integrated Client Firewall Scenario for Split Tunneling Configuration



Configuring Access Lists for a Client Firewall Configuration (CLI)

The CLI commands that configure the client access lists used in the example are as follows:

```
hostname(config)# access-list FWBlockIn deny ip any any
hostname(config)# access-list FWAllowAnyOut permit ip any any
hostname(config)# group-policy GroupPolicy4 attributes
hostname(config-group-policy)# client-firewall req cisco-integrated acl-in FWBlockIn
acl-out FWAllowAnyOut
```

The first **access-list** command can work as a default for blocking all inbound traffic to the VPN client. The identifier of the ACL is **FWBlockIn**. The action is **deny**, the protocol is **ip**, and the source address/mask and destination address/mask are both **any** (block all traffic from anywhere to the VPN client).

The second command allows all outbound traffic from the VPN client or groups of VPN clients. The identifier of this ACL is **FWAllowAnyOut**. The action is **permit**, the protocol is **ip**, and the source address/mask and destination address/mask are both **any** (let all traffic out from source to destination).

Configuring a Client Firewall in a Group Policy

This section gives both CLI and ASDM instructions to configure a client firewall as part of a group policy.

Using CLI Commands

You can use the **show running-config group-policy** *name* command to display the running configuration for a particular group policy.

To configure a firewall for VPN clients or groups of VPN clients for remote users, use the **group-policy** command. The syntax of the command used for this example is as follows:

group-policy *name* **attributes**

client-firewall opt | req cisco-integrated acl-in *ACL* **acl-out** *ACL*

The following commands create a group policy named GroupPolicy4 and enter config-group-policy mode to configure a client firewall requiring Cisco Integrated Firewall. The inbound ACL is FWBlockIn and the outbound ACL is FWAllowAnyOut. Using this example, you can finish setting up a default firewall policy.

```
hostname(config)# group-policy GroupPolicy4 attributes
hostname(config-group-policy)# client-firewall req cisco-integrated acl-in FWBlockIn
acl-out FWAllowAnyOut
```

Using ASDM

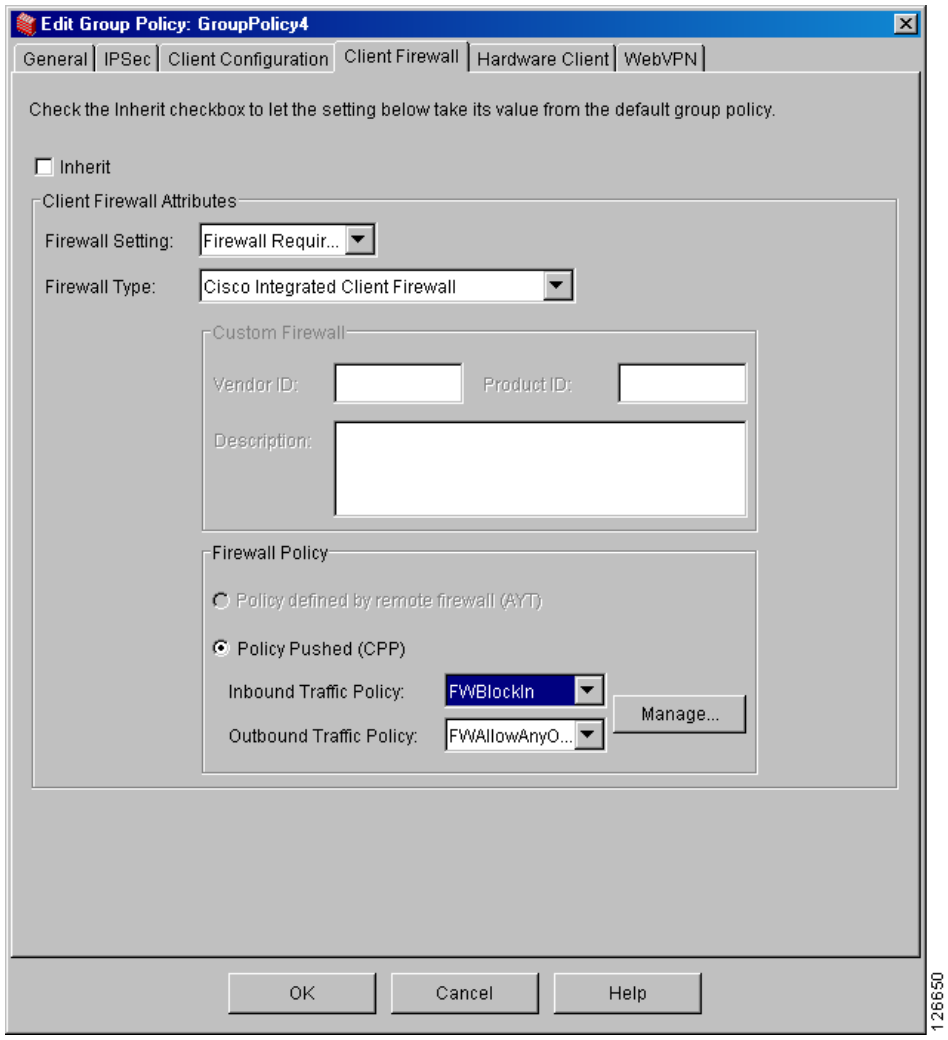
To configure client firewall protection using ASDM, add a group policy or edit an existing one. This example edits an existing policy named GroupPolicy4.

Step 1 Under the **Configuration > Features > VPN > General > Group Policy** panel, select the group policy in the table and click **Edit**. ASDM displays the **Edit Group Policy** dialog box.

Step 2 Click the **Client Firewall** tab. Figure 5-7 shows the client firewall options configured for this example:

- Inherit—**unchecked** (disabled)
- Firewall Setting**—Firewall Required**
- Firewall Type—**Cisco Integrated Client Firewall**
- Firewall Policy—**Policy Pushed (CPP)**

Figure 5-7 Client Firewall Options



Step 3 Click to uncheck the **Inherit** box.

Step 4 To select a firewall setting, click an option in the **Firewall Setting** list. This example configures **Firewall Required**. The list contains the following options.

- **No Firewall**—No firewall is required for remote users in this tunnel group. This is the default setting.
- **Firewall Required**—All remote users in this tunnel group must use a specific firewall. Only those users with the designated firewall can connect.

  If you choose **Firewall Required** as in this example, all users in the tunnel group must use the designated firewall. The ASA drops any session that attempts to connect without the designated, supported firewall installed and running. In this case, the ASA notifies the VPN client that its firewall configuration does not match.

Note If you require a firewall for a tunnel group, make sure the tunnel group does not include any clients other than Windows-based VPN clients. Any other clients in the tunnel group (including hardware clients) are unable to connect.

- **Firewall Optional**—All remote users in this tunnel group can connect. Those who have the designated firewall can use it. Those who do not have a firewall receive a warning message.

  If remote users in a tunnel group do not have firewall capacity, click **Firewall Optional**. The **Firewall Optional** setting lets all users in the tunnel group connect. Those who have a firewall can use it; those who connect without a firewall receive a warning message.

  This setting is useful if you are creating a tunnel group in which some users have firewall support and others do not—for example, you may have a tunnel group that is in gradual transition, in which some members have set up firewall capacity and others have not yet done so.

Step 5 Select a firewall from the **Firewall Type** list. This example specifies the **Cisco Integrated Client Firewall**.

Make sure that the firewall you designate correlates with the firewall policies available. The specific firewall you configure determines which firewall policy options are supported. (See Table 5-1 for details.)

Click one of the following:

- **Cisco Integrated Client Firewall**—The stateful firewall built into the Cisco VPN client.
- **Cisco Security Agent**—Cisco intrusion prevention (threat protection for server and desktop systems).
- **Custom Firewall**—A combination of the firewalls from the same vendor, or other firewalls not listed. If you choose this option, you must create your own list of firewalls in the **Custom Firewall** group box. Instructions to configure a custom firewall are not included in this guide.
- **Network ICE BlackICE Defender**—The Network ICE BlackICE Agent or Defender personal firewall.
- **Sygate Personal Firewall**
- **Sygate Personal Firewall Pro**
- **Sygate Security Agent**—The Sygate Security Agent personal firewall.
- **Zone Labs ZoneAlarm**—The Zone Labs ZoneAlarm personal firewall.
- **Zone Labs ZoneAlarm or ZoneAlarm Pro**—Either the Zone Labs ZoneAlarm personal firewall or the Zone Labs ZoneAlarm Pro personal firewall.
- **Zone Labs ZoneAlarm Pro**—The Zone Labs ZoneAlarm Pro personal firewall.

Step 6 To select a firewall policy, click an option in the **Firewall Policy** group box.

Depending on which firewall you configured, certain firewall policy options are available. (See Table 5-1.)

Table 5-1 Firewall Policy Options Available for Each Firewall

Firewall	Policy Defined by Remote Firewall (AYT)	Policy Pushed (CPP)
Cisco Integrated Client Firewall	No	Yes
Cisco Security Agent	Yes	No
Network ICE BlackICE Defender	Yes	No
Sygate Personal Firewall	Yes	No
Sygate Personal Firewall Pro	Yes	No
Sygate Security Agent	Yes	No

Table 5-1 Firewall Policy Options Available for Each Firewall

Firewall	Policy Defined by Remote Firewall (AYT)	Policy Pushed (CPP)
Zone Labs ZoneAlarm	Yes	Yes
Zone Labs ZoneAlarm or Zone Labs ZoneAlarm Pro	Yes	Yes
Zone Labs ZoneAlarm Pro	Yes	Yes

Step 7 Select from the options associated with the firewall policy.

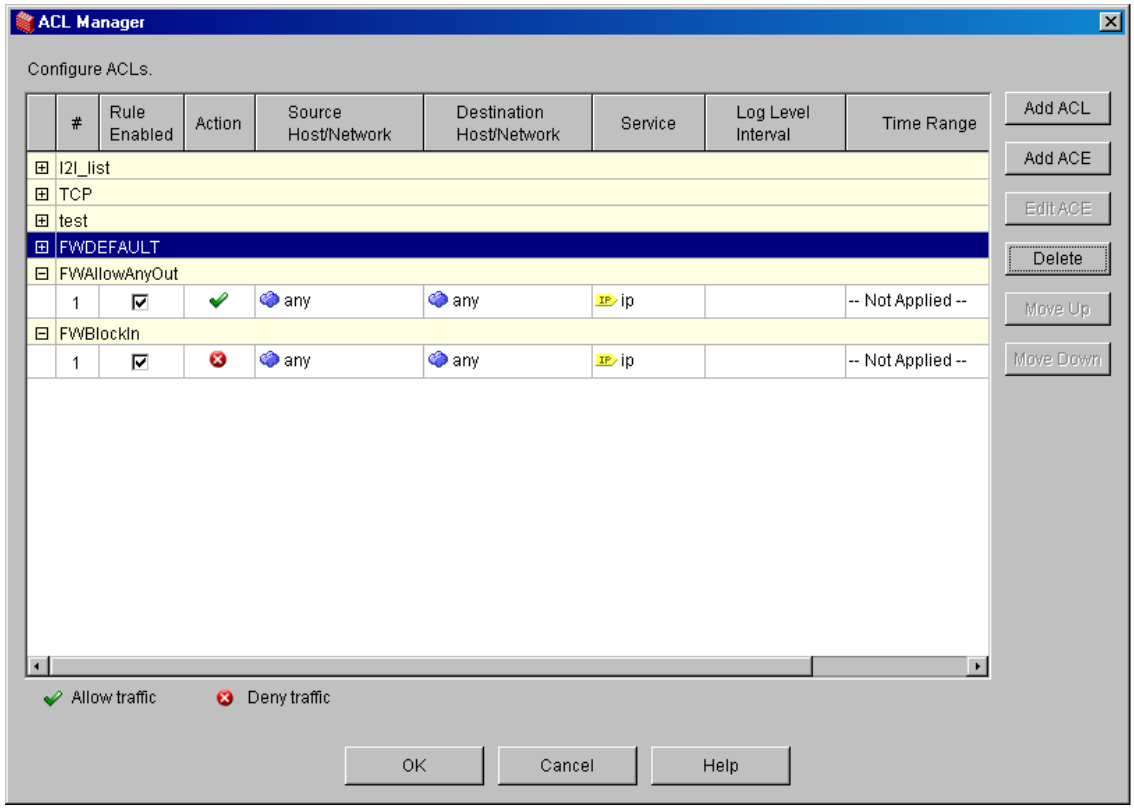
This example specifies **Policy Pushed (CPP)**. The **Firewall Policy** list contains the following options:

- **Policy defined by remote firewall (AYT)** —Remote users in this tunnel group have firewalls located on their PCs. The local firewall enforces the firewall policy on the VPN client. The ASA allows VPN clients to connect only if they have the designated firewall installed and running. If the designated firewall is not running, the connection fails. Once the connection is established, the VPN client polls the firewall every 30 seconds to make sure that it is still running. If the firewall stops running, the VPN client ends the session.
- **Policy Pushed (CPP)** —The ASA enforces on the VPN clients the traffic management rules defined by the ACLs you choose from the Policy Pushed (CPP) lists:
  - **Inbound Traffic Policy**—Select an ACL to control inbound traffic to the VPN client.
  - **Outbound Traffic Policy**—Select an ACL to control outbound traffic from the VPN client.

  If the VPN client also has a local firewall, the policy pushed from the ASA coexists with the policy of the local firewall. Any packet that is blocked by the rules of *either* firewall is dropped.

Step 8 If you have selected CPP, click an ACL in the **Inbound Traffic Policy** list and also in the **Outbound Traffic Policy** list. ASDM does not let you choose the same ACL for both lists. To add ACLs to either list, click **Manage**. The ASDM displays the **ACL Manager** table. This example adds two ACLs, one to use as the inbound traffic policy and the other to use as the outbound traffic policy (see Figure 5-8).

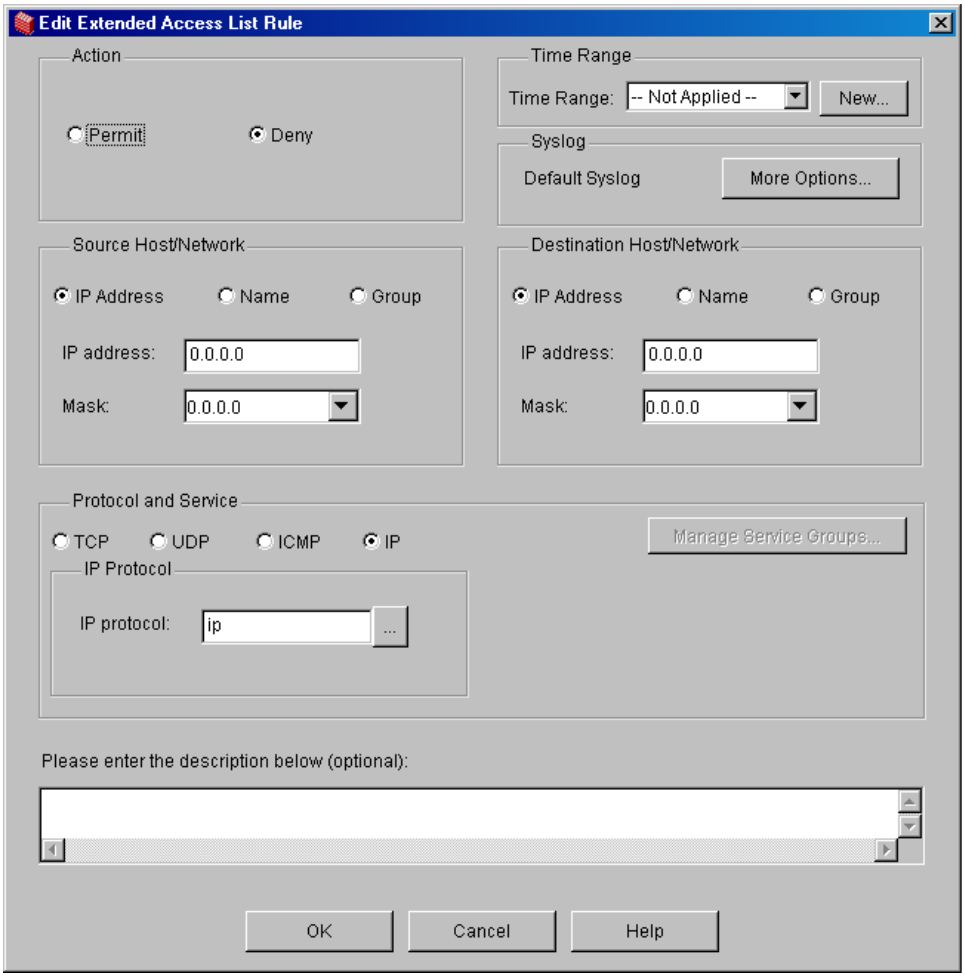
Figure 5-8 Using the ACL Manager



Step 9 To add an ACL, click **Add ACL**, type a name for the ACL in the **ACL ID** box and click **OK**. For the inbound ACL, the name is FWBlockIn as the identifier.

Step 10 Click the **FWBlockIn** ACL you just added and then click **Add ACE** to insert an Access Control Entry. The **Add Extended Access List Rule** dialog box appears. For information on all the fields, click **Help** (See Figure 5-9).

Figure 5-9 Adding an Access List Rule



a. For CPP policy, you need to deny all traffic from unsolicited networks and hosts to the VPN client or group of VPN clients. To accomplish this, click the **Deny** option. For the source host/network and destination host/network, accept the defaults **0.0.0.0** (any).

b. To configure IP as the default protocol, in the **Protocol and Service** group box, click the **IP** option. The default service is **any** for both source and destination. To change these, click **Help** for more information.

Step 11 Following the same procedure, add the second ACL to permit all outgoing traffic from the VPN clients.

a. Type **FWAllowAnyOut** in the **ACL ID** box.

b. Click **Add ACE** , and when the **Add/Edit Extended Access List Rule** dialog box displays, click **Permit** as the **Action** and **IP** as the **Protocol**.

Step 12 Click **OK**. ASDM displays the **ACL Manager** where you can see that the ACLs have been added. See Figure 5-8.

Step 13 Click **OK** again. ASDM displays the **Client Firewall** tab.

Step 14 Under the **Policy Pushed (CPP)** option, configure the inbound and outbound traffic policies.

a. In the **Inbound Traffic Policy** list, click **FWBlockIn**.

b. In the **Outbound Traffic Policy** list, click **FWAllowAnyOut**.

c. Click **OK**. ASDM displays the **Group Policy** panel.

Step 15 Click **Apply** and then save configuration.

Configuring a Client Firewall to Allow HTTP Traffic

You can set up a client firewall to allow HTTP traffic in and block all other incoming traffic. In this example, you use the FWAllowAnyOut created in the previous section as the outbound traffic policy.

Using CLI Commands

To allow HTTP traffic and deny all other inbound traffic, execute the following **access-list** commands in configuration mode. The name of the ACL is FWAllowHTTP, TCP is the protocol in use, and the port number for HTTP traffic is 80.

Step 1 Set up the ACLs. The first two commands define the inbound traffic policy and the third command defines the outbound traffic policy:

```
hostname(config)# access-list FWAllowHTTP permit tcp any any eq 80
hostname(config)# access-list FWAllowHTTP deny ip any any
hostname(config)# access-list FWAllowAnyOut permit ip any any
```

Step 2 Enter the client-firewall command in group-policy mode. The name of the group policy for this example is ClientServer.

```
hostname(config)# group-policy ClientServer internal
hostname(config)# group-policy ClientServer attributes
hostname(config-group-policy)# client-firewall req cisco-integrated acl-in FWAllowHTTP
acl-out FWAllowAnyOut
```

Using ASDM

Using ASDM, configure the Cisco Integrated Client Firewall and CPP as follows:

Note For more information, see "Configuring a Client Firewall in a Group Policy."

Step 1 Under **Configuration > Features > VPN > General > Group-Policy**, add or edit a group policy. This example adds a new policy called **ClientServer**.

a. Click **Add** and type **ClientServer** in the **Name** box.

b. Accept the default **internal**.

Step 2 Click the **Client Firewall** tab.

Step 3 Click the **Inherit** option to uncheck it.

Step 4 Click the **Firewall Required** option in the **Firewall Setting** list.

Step 5 Keep **Cisco Integrated Client Firewall** as the **Firewall Type**.

This setting automatically enables the **Policy Pushed (CPP)** option under the **Firewall Policy** group box.

Step 6 Click **Manage**.

Step 7 Click **Add ACL** and type the name **FWAllowHTTP** in the **ACL ID** box.

Step 8 Click **FWAllowHTTP** in the table and click **Add ACE**. Configure the following options:

a. Under **Action**, use the default option (**Permit**).

b. Use the default **Protocol and Service** setting (**TCP**). This option enables the **Service** parameter below it.

c. Use the default **Service** operator (**=**) on the left, click **...**, click **http** in the list that displays, and click **OK**.

d. On the **Destination Port** side, keep the default **Service = any** settings.

e. Click **OK**.

Step 9 Click **OK**.

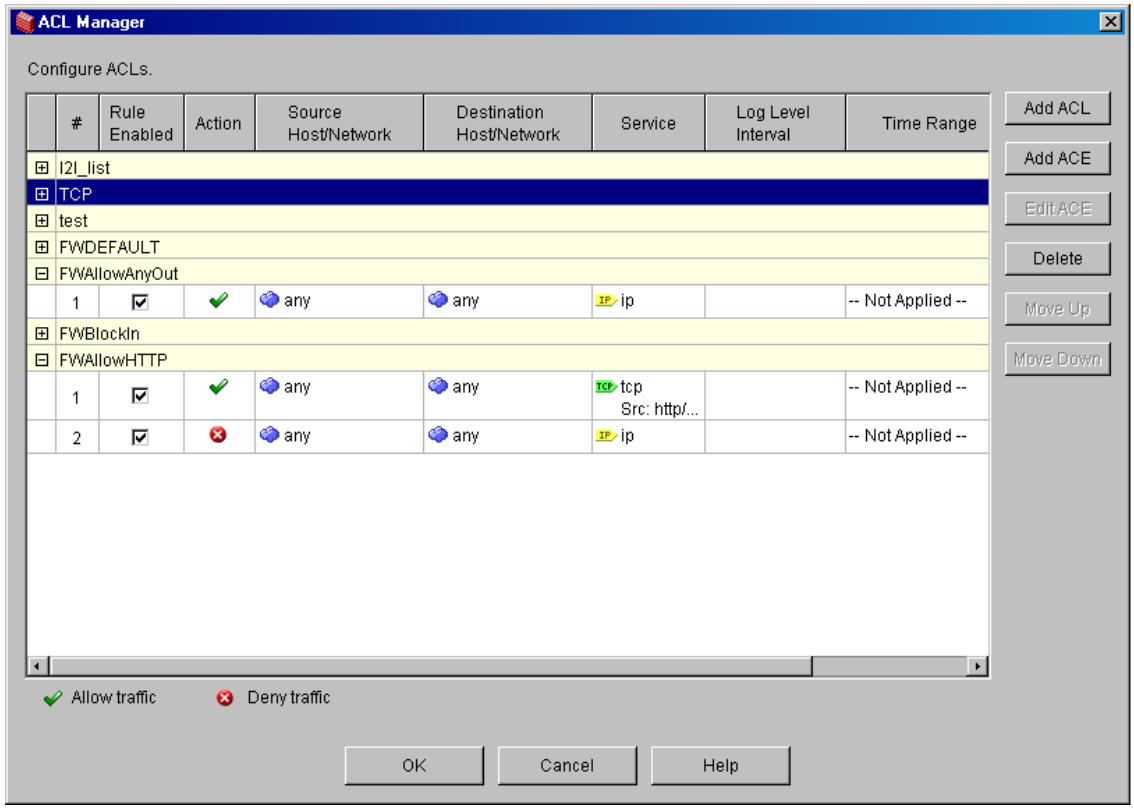
Step 10 On the **Client Firewall** tab, under **Firewall Policy** and **Policy Pushed (CPP)**, click **FWAllowHTTP** in the **Inbound Traffic Policy** list and click **FWAllowAnyOut** in the **Outbound Traffic Policy** list. Then click **Manage**.

Step 11 In the **ACL Manager** table, under the **FWAllowHTTP ACL**, click **Add ACE** to add the second rule.

The steps adds another rule under **FWAllowHTTP** to **deny** all traffic. (The rule goes after the rule that permits HTTP traffic).

Step 12 Under **Action**, click **Deny**, under **Protocol and Service**, click **IP** and then click **OK**. Figure 5-10 shows the resulting configuration in the **ACL Manager** table for this example. Note that the **FWAllowHTTP** ACL has two rules in the correct order. Traffic inbound to the VPN Client from HTTP can get through but all other traffic is denied.

Figure 5-10 Client Firewall ACLs for Using the VPN Client as a Web Server



Step 13 On the **Client Firewall** tab, click **OK** again and then click **Apply**.

Authenticating with External Servers

This example shows how to configure external authentication for remote-access users, specifically how to configure a RADIUS server.

Overview of Configuration Procedure

To configure external authentication, use the following procedure:

1. Create an AAA server group for authentication.
2. Add hosts to the AAA server group.
3. Add or edit a remote-access tunnel group for external authentication.

This example uses the following scenario:

- The name of the AAA server group is ACSRadiusServer.
- The IP addresses of the AAA hosts are: 172.16.0.1, 172.16.0.2, and 172.16.0.3.
- The name of the remote-access tunnel group is ACSRadiusGroup.

Creating an IP Address Pool

The first step is creating an IP address pool for VPN clients calling in. Alternatively, you can also use a DHCP server for distributing IP addresses to clients. This example uses an address pool.

Using CLI Commands

To create an IP address pool, use the **ip local pool** command. The syntax of the command is:

ip local pool *poolname* *first-address—last-address* [**mask** *mask*]

For example, enter the following command to create an IP address pool named IPPool2 with an address range from 10.20.30.40 to 10.20.30.60:

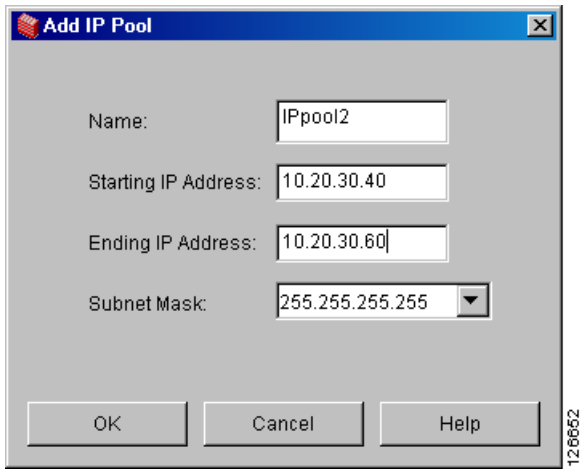
```
hostname(config)# ip local pool IPPool2 10.20.30.40-10.20.30.60
hostname(config)#
```

Using ASDM

To create an IP address pool:

Step 1 Under **Configuration > Features > VPN > IP Address Management > IP Pools**, click **Add**. ASDM displays the **Add IP Pool** dialog box (see Figure 5-11).

Figure 5-11 Adding an IP Address Pool



Step 2 Type the name for the IP pool in the **Name** text box. For this example the name is IPpool2.

Step 3 Type the starting IP address in the **Starting IP Address** text box. For this example the starting IP address is 10.20.30.40.

Step 4 Type the ending IP address in the **Ending IP Address** text box. For this example the ending IP address is 10.20.30.60.

Step 5 Click a subnet mask in the **Subnet Mask** list. In ASDM, configuring the subnet mask is required.

Step 6 Click **OK** and then click **Apply**.

Adding a Server Group

Add an external server group for authentication. This example adds a server group for RADIUS authentication named ACSRadiusServers using the following features:

- RADIUS protocol
- Single accounting mode
- Timed reactivation mode

  This options reactivates the server after 30 seconds of down time. The default setting is depletion, which reactivates failed servers only after all of the servers in the group are inactive.
- Number of failed attempts before deactivating the server is 2

  The default value is 3.

Using CLI Commands

To configure a server group, use the **aaa-server protocol** command. The syntax of the **aaa-server protocol** command that configures this server group as a RADIUS server group is:

aaa-server *server-tag* **protocol** *server-protocol*

When you enter the aaa-server command, the CLI puts you in config-aaa-server-group mode for configuring AAA server group attributes.

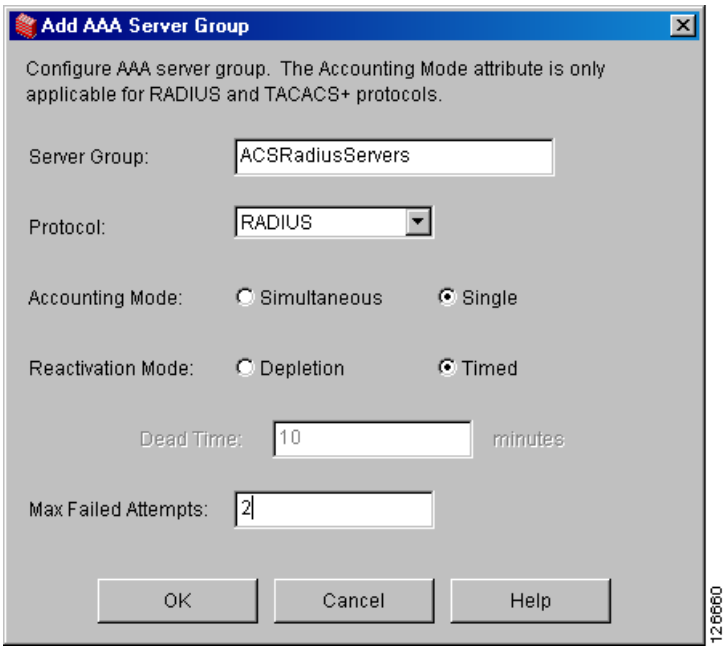
The following commands configure a AAA server group named RadiusServer that uses the RADIUS protocol.

```
hostname(config)# aaa-server ACSRadiusServers protocol radius
hostname(config-aaa-server-group)# accounting-mode single
hostname(config-aaa-server-group)# reactivation-mode timed
hostname(config-aaa-server-group)# max-failed-attempts 2
```

Using ASDM

Step 1 To configure server groups for authentication, under the **Configuration > Features > Properties > AAA Setup > AAA Server Groups** panel, click **Add**. ASDM displays the **Add AAA Server Group** dialog box (see Figure 5-12).

Figure 5-12 Adding an AAA Server Group



Step 2 Enter the information for the server group you are adding:

a. **Server Group**—Type a name for this server group. For this example, the name is **ACSRadiusServers**.

Protocol—Click the protocol that this server group uses in the Protocol list. You can choose from the following protocols. For this example, the protocol is RADIUS.

- **RADIUS**
- **TACACS+**
- **NT Domain**
- **SDI**
- **Kerberos**
- **LDAP**

b. **Accounting Mode**—For RADIUS or TACACS+, click an accounting mode option: **Simultaneous** or **Single** (the default). In simultaneous mode, the ASA sends accounting data to all servers in the group. In single mode, the ASA sends accounting data to only one server. This example accepts the default Single.

c. **Reactivation Mode**—The way failed servers are reactivated: **Depletion** or **Timed**. In Depletion mode, failed servers are reactivated only after all servers in the group are inactive. In timed mode, failed servers are reactivated after 30 seconds of down time. Click one of these options. The default is Depletion. This example uses timed as the reactivation mode.

d. **Dead Time**—When the reactivation mode is Depletion, you must configure the number of minutes to elapse between disabling the last server in the group and reenabling all servers. The default is 10.

e. **Max Failed Attempts**—The number of failed connection attempts allowed before declaring a nonresponsive server dead. Type the number of attempts to allow. The default is 3. This example sets the value to 2.

Step 3 Click **OK** and then click **Apply**.

Adding a AAA Hosts to the AAA Server Group

Once you configure an AAA server group, you can add AAA hosts (in this case RADIUS servers) to the server group by identifying the IP address of each host you are adding to the group, and identifying the interface that the host is using (optional).

Using CLI Commands

In CLI, this example adds three hosts to the server group ACSRadiusServers on the inside interface. These commands define the host IP address and show the parameters you can configure in aaa-server-group mode.

This syntax for the **aaa-server host** command is:

aaa-server *server-tag* [(*interface-name*)] **host** *server-ip*

The example **aaa-server host** commands used to add the AAA server hosts reference the following attributes:

- **retry-interval**—Number of seconds to wait before attempts to connect. The default value is 10.
- **timeout**—Number of minutes after which the ASA gives up on the request to the primary AAA server and sends it to the backup server if there is one. The default value is 10.
- **key**—case sensitive encryption key.

```
hostname(config)# aaa-server ACSRadiusServers (inside) host 172.16.0.1
```

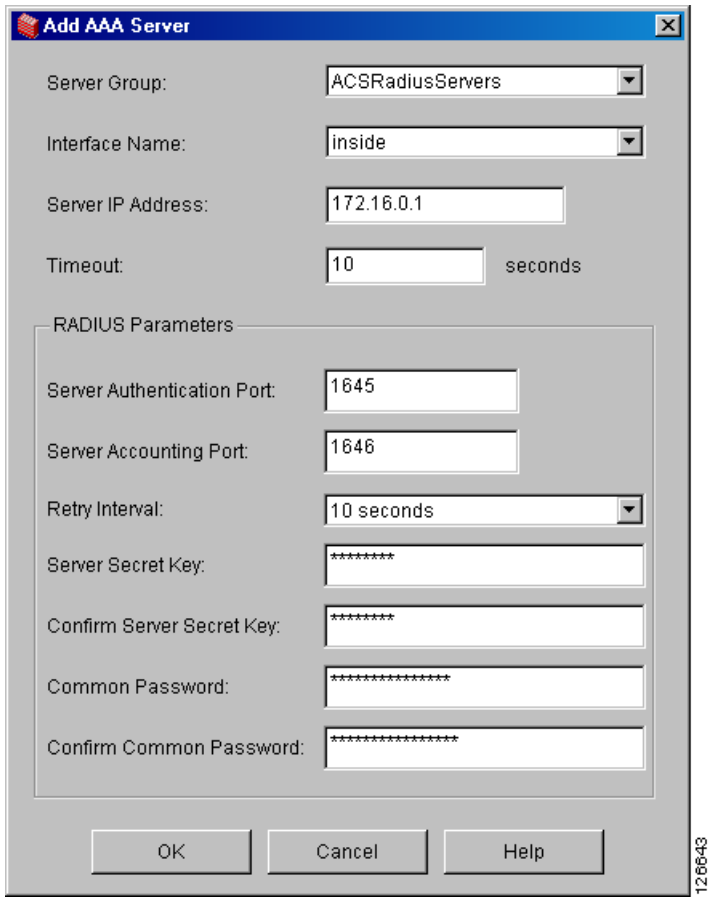
```
hostname(config-aaa-server-group)# retry-interval 5
hostname(config-aaa-server-group)# timeout 16
hostname(config-aaa-server-group)# key x5*zbrct
hostname(config-aaa-server-group)#
hostname(config)# aaa-server ACSRadiusServers (inside) host 172.16.0.2
hostname(config-aaa-server-group)# retry-interval 5
hostname(config-aaa-server-group)# timeout 16
hostname(config-aaa-server-group)# key x5*zbrct
hostname(config-aaa-server-group)#
hostname(config)# aaa-server ACSRadiusServers (inside) host 172.16.0.3
hostname(config-aaa-server-group)# retry-interval 5
hostname(config-aaa-server-group)# timeout 16
hostname(config-aaa-server-group)# key x5*zbrct
hostname(config-aaa-server-group)#
```

Using ASDM

Use ASDM to add an AAA server to the AAA server group using RADIUS for authentication, as follows:

Step 1 Under the **Configuration > Features > Properties > AAA Setup > AAA Servers** panel, click **Add**. ASDM displays the **Add AAA Server** dialog box. Figure 5-13 shows this dialog box configured with values for this example.

Figure 5-13 Adding an AAA Server for External Authentication



Step 2 For the first host in the group, enter following information:

a. **Server Group**—Select the name of the **AAA Server** from the **Server Group** list. For this example, select **ACSRadiusServer**, the server group added in "Adding a Server Group."

b. **Interface Name**—Select the name of the network interface associated with the authentication server from the **Interface Name** list. For this example, select **inside**.

c. **Server IP Address**—Type the IP address of the AAA server. For this example, the IP address of the first host to add is 172.16.0.1.

d. **Timeout**—Type the number of minutes after which the ASA should give up on the request to the primary AAA server and sends the request to the backup server if there is one. For this example, use the default setting, 10 seconds.

e. **RADIUS Parameters** group—Configure the parameters in this group box. For this example, accept defaults where they exist. You must supply the server's secret key and the common group password.

Note Only RADIUS servers use a common password.

f. **Retry Interval**—Select the number of seconds to wait before attempts to connect. The default setting is 10 seconds. For this example, use the default setting.

g. **Server Authentication Port**—The server port for user authentication. The default port is 1645.

h. **Server Accounting Port**—The server port for user accounting. The default port is 1646.

i. **Server Secret Key**—Type the encryption key, which is case sensitive. For this example, the key is x5*zbrct.

j. **Confirm Secret Key**—Type the secret key again in this text box.

Step 3 After specifying the settings, click **OK** and **Apply**.

Following the same procedure, add the remaining two hosts to the AAA server groups.

Adding a Tunnel Group for Remote Access Using External Authentication

Finally, add a tunnel group. For this example, the name of the tunnel group is ACSRadiusGroup. The name of the AAA server group is ACSRadiusServers.

Using CLI Commands

The following commands name a tunnel group, access the tunnel-group general attributes mode, and assign the tunnel group to the authentication group. The last two commands enter IPSec attributes mode and configure the preshared key for remote access authentication.

```
hostname(config)# tunnel-group ACSRadiusGroup type ipsec_ra
hostname(config)# tunnel-group ACSRadiusGroup general-attributes
hostname(config-general)# address-pool IPPool2
hostname(config-general)# authentication-server-group ACSRadiusServers
hostname(config)# tunnel-group ACSRadiusGroup ipsec-attributes
hostname(config-ipsec)# pre-shared k*5$h9s%
```

Using ASDM

Use ASDM to add a tunnel group for remote access with external authentication, as follows:

Step 1 Under the **Configuration > Features > VPN > General > Tunnel Group** panel, click **Add**. ASDM displays the **Add Tunnel Group** dialog box showing the **Identity** tab.

Step 2 Type a name for this tunnel group in the **Name** text box and click the **IPSec for Remote Access** option in the **Type** group box. For this example, the name is ACSRadiusGroup.

Step 3 Click the **General** tab and select the server group from the **Authentication Server Group** list. For this example, the name of the server group is **ACSRadiusServers** (see "Adding a Server Group").

Step 4 To configure IPSec attributes for this remote-access tunnel group, click the **IPSec** tab and type the encryption key in the **Pre-shared Key** text box. For this example, the preshared key is k*5$h9s%. Then click **OK** and **Apply**.

Configuring Traffic Management

This chapter describes the following configuration tasks:

Configuring Load Balancing

If you have a remote-client configuration in which you are using two or more ASAs connected on the same network to handle remote sessions, you can configure those devices to share their session load. This feature is called *load balancing*. Load balancing directs session traffic to the least loaded device, thus distributing the load among all devices. It makes efficient use of system resources and provides high availability.

To implement load balancing, group together logically two or more devices on the same subnet into a *virtual cluster.*

All devices in the virtual cluster carry session loads. One ASA in the virtual cluster, the *virtual cluster master*, can accept connections and also direct incoming calls to the other devices, called *backup devices*. The virtual cluster master monitors all devices in the cluster, keeps track of how busy each is, and distributes the session load accordingly. The role of virtual cluster master is not tied to a physical device; it can shift among devices. For example, if the current virtual cluster master fails, one of the backup devices in the cluster takes over that role and immediately becomes the new virtual cluster master.

To outside clients, the virtual cluster appears as a single *virtual cluster IP address*. This IP address is not tied to a specific physical device. It belongs to the current virtual cluster master; hence, it is virtual. A VPN client attempting to establish a connection connects first to this virtual cluster IP address. The virtual cluster master then sends back to the client the public IP address of the least-loaded available device in the cluster. In a second transaction (transparent to the user), the client connects directly to that device. In this way, the virtual cluster master directs traffic evenly and efficiently across resources.

If a device in the cluster fails, the terminated sessions can immediately reconnect to the virtual cluster IP address. The virtual cluster master then directs these connections to an active device in the cluster. Should the virtual cluster master itself fail, a backup device in the cluster immediately and automatically takes over as the new virtual session master. Even if several devices in the cluster fail, users can continue to connect to the cluster as long as any one device in the cluster is up and available.

Note For load balancing to work for WebVPN, all devices in the cluster must support WebVPN.

Prerequisites

Load balancing is disabled by default. You must explicitly configure and enable it.

Before you can configure load balancing, the public and private interfaces must be configured and the interface for the virtual cluster IP address must be defined.

All devices in the cluster must share the same cluster-specific values:

- Virtual cluster IP address
- Encryption settings (optional)
- Encryption key (optional unless Encryption is enabled)
- Port identifier (the default UDP is 9023)

Overview of Configuration Procedure

To configure a minimal VPN load balancing scheme:

1. Define the virtual cluster IP address, the IP address to be shared by all devices in the VPN load balancing cluster. The address must be within the public subnet address range shared by the devices.
2. If configuring stateful failover, enable encryption and define an encryption key to be shared by all devices in the cluster. The devices in the virtual cluster communicate via LAN-to-LAN tunnels using IPSec. Enabling encryption ensures that all load-balancing information communicated between them is encrypted.
3. Optionally change the default priority of a device within the cluster. The range is from 1 to 10; 10 is the highest. The priority indicates the likelihood of the device becoming the virtual cluster master, either at start-up or when an existing master fails. The higher you set the priority, the more likely this device becomes the virtual cluster master.
4. Enable load balancing on each ASA included in the cluster.

The example in this section configures the following values:

- Cluster IP address is 209.165.202.224.
- Cluster encryption key is 12345678.
- Encryption is enabled on this cluster.
- The ASA in this example has a priority of 10.

The example in this section uses the following CLI commands to configure load balancing.

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# priority 10
hostname(config-load-balancing)# cluster key 12345678
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)# participate
```

Using CLI Commands

You can enter the **show running-config vpn load-balancing** command to display the running configuration for a particular group policy.

Use the CLI to configure load balancing as follows:

Step 1 When you execute the **vpn load-balancing** command, the CLI puts you in config-load-balancing mode, where you configure the cluster parameters. In this mode, enter the **cluster** command to configure the virtual cluster IP address, as follows:

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# cluster ip address 209.165.202.224
```

Step 2 To use encryption in this configuration, use **cluster** commands to define the encryption key and then enable encryption. This step is optional. You must configure the encryption key before you enable encryption.

```
hostname(config-load-balancing)# cluster key 12345678
hostname(config-load-balancing)# cluster encryption
```

Step 3 (Optional) To change the default priority of the ASA, use the **priority** command, as follows:

```
hostname(config-load-balancing)# priority 10
```

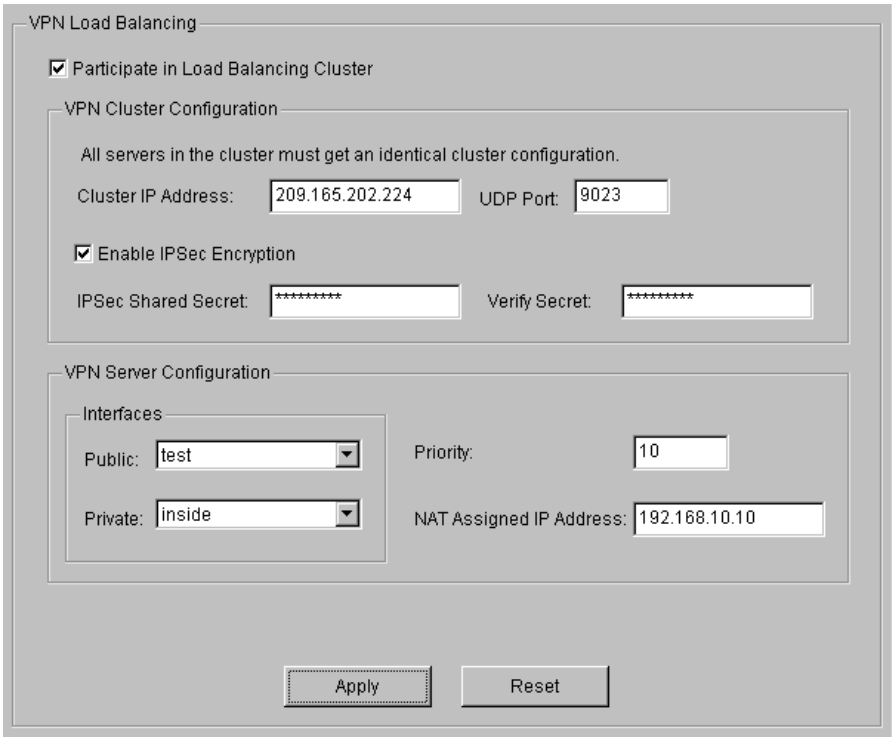
Step 4 To enable load balancing on this ASA, use the **participate** command, as follows:

```
hostname(config-load-balancing)# participate
```

Using ASDM

The following procedure shows how to use ASDM to configure load balancing. Note that many of the parameters in this example have default values.

Figure 6-1 Configuring Load Balancing in ASDM



Step 1 To enable VPN load balancing, go to **Configuration > Features > VPN > Load Balancing**, and click **Participate in Load Balancing Cluster**.

Step 2 In the **VPN Cluster Configuration** group box, configure the parameters for all ASAs participating in the cluster, as follows:

- **a.** Type the IP address of the cluster in the **Cluster IP Address** text box.
- **b.** Click the **Enable IPSec Encryption** option.
- **c.** Type the encryption key in the **IPSec Shared Secret** text box and type it again in the **Verify Secret** text box.

Step 3 Configure the options in the **VPN Server Configuration** group box:

- **a.** In the **Public** list, select an interface that will accept the incoming VPN connections.
- **b.** In the **Private** list, select an interface that is the private interface.
- **c.** (Optional) Change the priority that the ASA has in the cluster in the **Priority** text box.
- **d.** If this device is behind a firewall using NAT, type an IP address for the **NAT Assigned IP Address**. For this example, the NAT assigned IP address is 192.168.10.10. If the device is not using NAT or if the ASAs are not behind a firewall using NAT, enter 0.0.0.0.

Configuring Quality of Service for VPN Traffic

The VPN 3000 Concentrator implemented bandwidth management as a part of traffic policy management. QoS, a component of the security policy configuration of the ASA, supersedes that implementation. In the ASA, the implementation of QoS is based on the IOS implementation of that feature.

QoS is a traffic-management strategy that lets you allocate network resources for both mission-critical and normal data, based on the type of network traffic and the priority you assign to that traffic. In short, QoS ensures unimpeded priority traffic or provides the capability of rate-limiting (policing) traffic.

QoS provides maximum rate control, or policing, on each individual user tunnel and site-to-site tunnel. (Individual user traffic within a tunnel is not taken into consideration for LAN-to-LAN connections.) This release does not provide a minimum bandwidth guarantee (bandwidth reservation).

Because QoS can consume large amounts of resources, which could degrade ASA performance, QoS is disabled by default.

The following sections show briefly how to use QoS to configure priority traffic for tunnel groups only.

Note Refer to *Cisco Security Appliance Command Line Configuration Guide* for complete information about QOS.

Overview of Configuration Procedure

Use ASDM to configure QoS as follows:

1. Configure a service policy.

   There can be only one service policy per interface or at the global level.
2. Configure the traffic classification criteria for the service policy rule.
3. Configure actions on the traffic classified by the service policy rule.

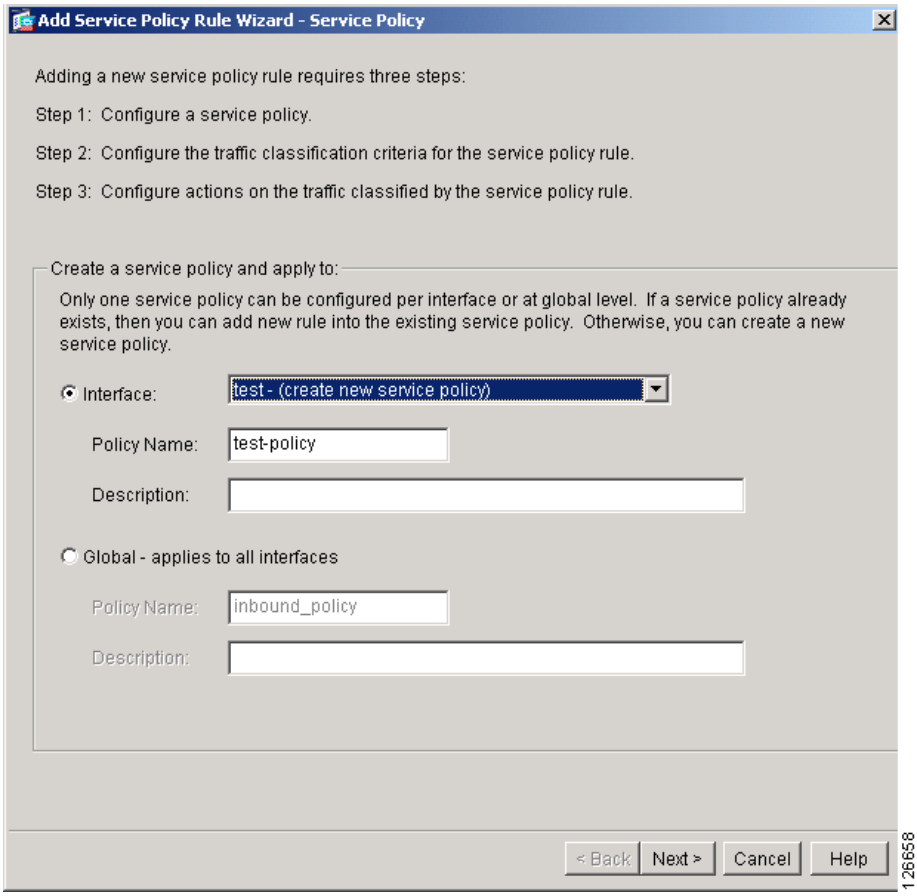
Using ASDM

ASDM provides a wizard to guide you through the steps for configuring QoS. This section shows how to use this wizard to configure QoS for a tunnel group. The ASDM **Help** button provides additional information.

Step 1 Under the **Configuration > Features > Security policy** panel, click **Service Policy Rules**.

Step 2 Click **Add**. ASDM displays the **Add Service Policy Rule Wizard - Service Policy** dialog box. Use this dialog box to create or edit a service policy.

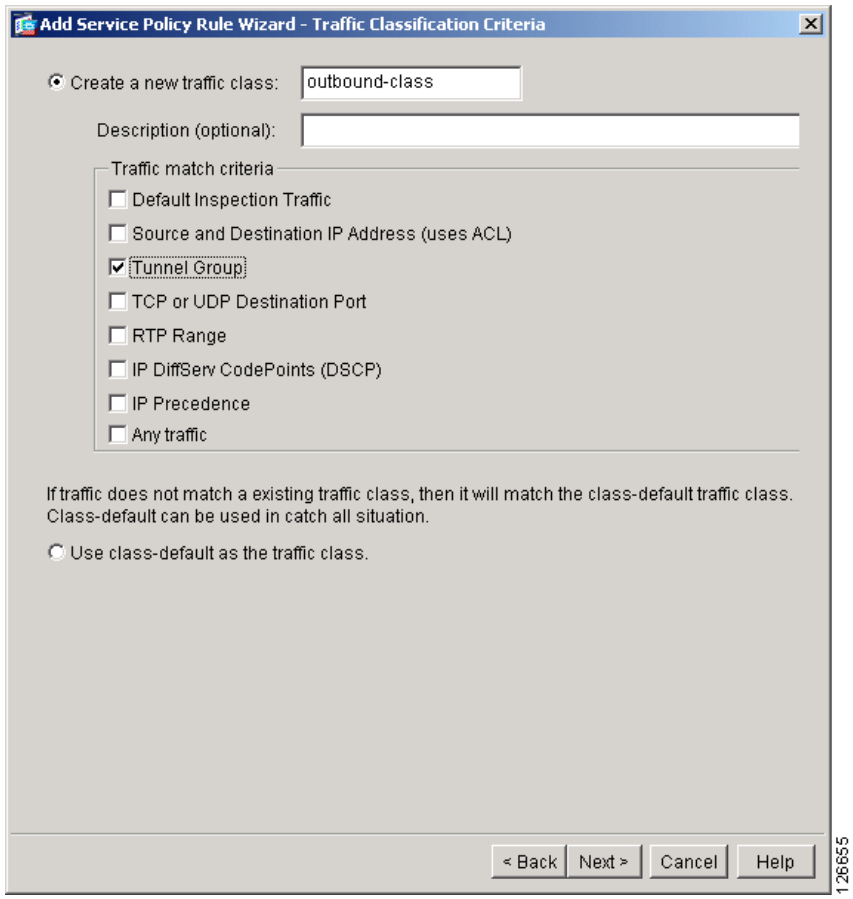
Figure 6-2 **Add Service Policy Rule Wizard - Service Policy Wizard**



Step 3 This example creates a new service policy and applies it to the test interface. To start, click the **Interface** option and then select the name **test - (create new service policy)** from the **Interface** list. (The text (create new service policy) is appended to the name of the interface).

Step 4 Type a name for the policy in the **Policy Name** text box. ASDM provides a default name by appending the word "policy" to the interface name. For this example, change it to outbound-policy. Click **Next**. ASDM displays the **Add Service Policy Rule Wizard - Traffic Classification Criteria** dialog box.

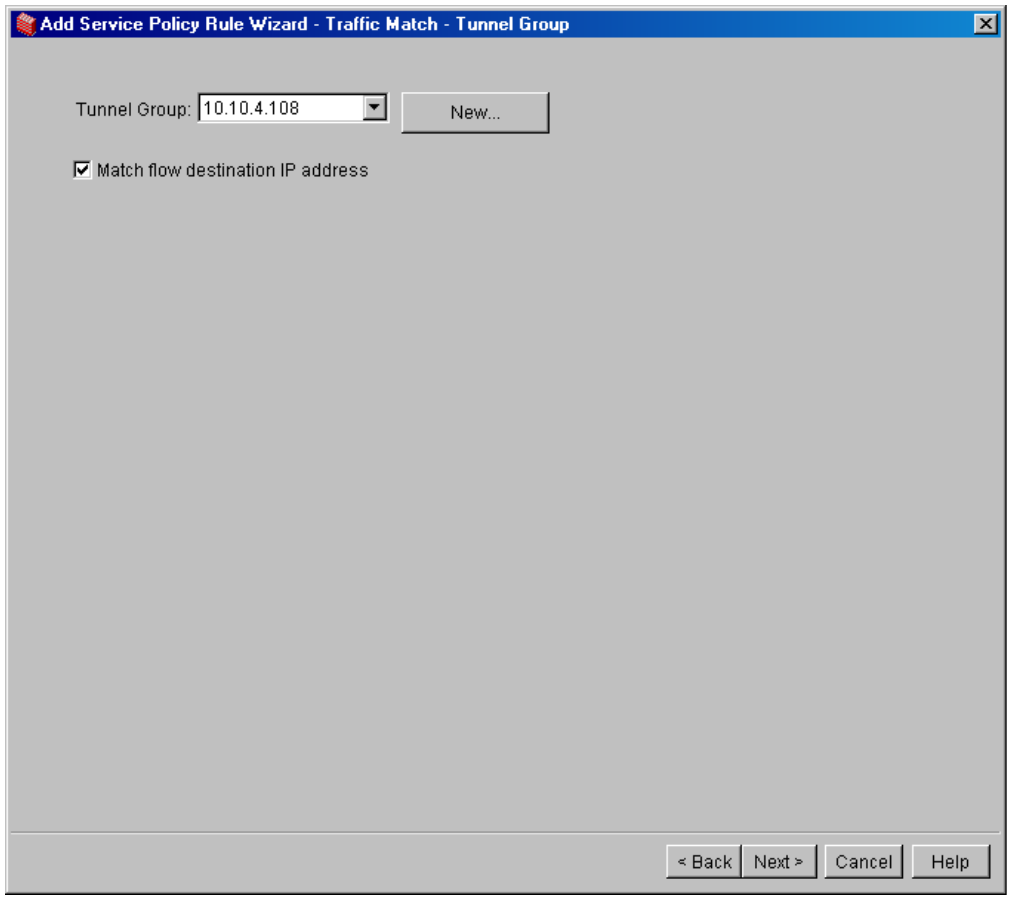
Figure 6-3 Add Service Policy Rule Wizard - Traffic Classification Criteria



Step 5 Click the **Create a new traffic class** option. ASDM combines the interface name with the word "class" to create a default policy name in the text box. For this example, change the name to outbound-class.

Step 6 The **Traffic match criteria** group box displays a subset of the match criteria that the ASA offers. For this example, click the **Tunnel Group** option and click **Next**. ASDM displays the **Add Service Policy Rule Wizard-Traffic Match - Tunnel Group** dialog box.

Figure 6-4 Add Service Policy Rule Wizard-Traffic Match - Tunnel Group

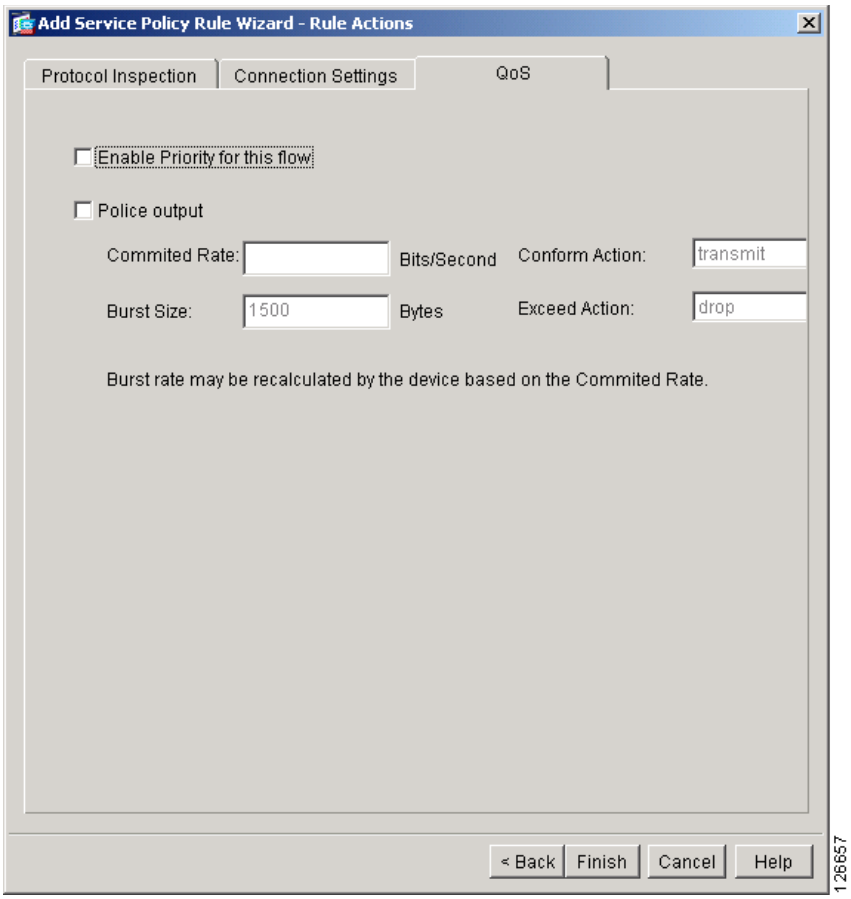


Step 7 Select the IP address of a tunnel group already in the system or click **New** to configure a new tunnel group. For this example, select an **10.10.4.108** from the **Tunnel Group** list and click **Match flow destination IP address**. Enabling this option applies the traffic action to be selected in the next dialog box to this tunnel group. Click **Next**.

ASDM displays the **Add Service Policy Rule Wizard - Rule Actions** dialog box.

Step 8 Click the **QoS** tab.

Figure 6-5 Configuring QoS Options



The QoS tab lets you select one of the following rule actions:

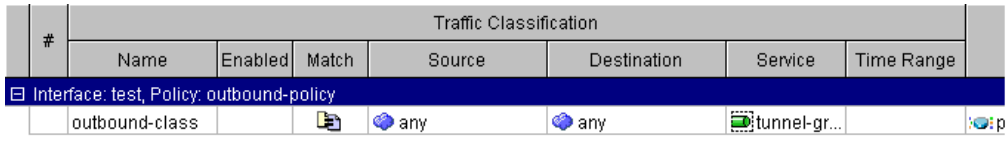
- **Enable Priority for this flow**—Make traffic to this tunnel-group a priority.
- **Police output**—Establish criteria for policing the traffic going to this tunnel group. If you enable this option, change the values for committed rate, burst rate, conform action and exceed action, or accept the default values. For definitions of these parameters, click **Help**.

Step 9 To establish priority queuing for this tunnel group, click **Enable Priority for this flow** and **Finish**.

Step 10 Click **Apply**.

Figure 6-6 shows the QoS security policy configured for this example.

Figure 6-6 QoS Policy Configured



Using CLI Commands

You can enter the **show running-config all service-policy** command to display the running service policy configuration for a particular group policy.

The following commands provide an example of how to use the CLI to configure priority traffic for tunnel groups. (Note that the command sequence is different from the wizard described in the previous section.)

```
class-map outbound-class
  match tunnel-group 10.10.4.108
  match flow-ip destination-address
policy-map outbound policy
  class outbound-class
    priority
service-policy outbound-policy interface test
```

Note For detailed instructions on how to configure QoS with the CLI, see *Cisco Security Appliance Command Line Configuration Guide*.

Mapping Topics from VPN 3000 Series Concentrators to ASDM

The following tables map the VPN 3000 Concentrator tasks to the Adaptive Security Device Manager paths:

- Table A-1, "Navigation Map for Configuration Tasks"
- Table A-2, "Navigation Map for Administration Tasks"
- Table A-3, "Monitoring Tasks"

Table A-1 Navigation Map for Configuration Tasks

VPN 3000 Task	Topic	ASDM Path
Using the VPN 3000 Management application	Not applicable	ASDM Online Help > Welcome to ASDM
Configuring Interfaces	Not applicable	Configuration > Features > Interfaces > Add
	power	Enable Interface/Dedicate to management only
	Ethernet	Hardware Port
	General parameters	VLAN ID/Sub-interface ID
Configuring Servers	AAA Servers	Configuration > Features > Properties > AAA Setup > AAA Server Groups
	authentication, authorization, and accounting	Configuration > Features > Device Administration > AAA Access
	DHCP	Configuration > Features > Properties > DHCP Services > DHCP Server and DHCP Relay
	DNS	Configuration > Features > Properties > DNS Client
	NTP	Configuration > Features > Device Administration > Administration > NTP
	External servers (TACACS and RADIUS)	Configuration > Features > Properties > AAA Setup > AAA Server Groups > Add AAA Server Group (Protocol list box)
Configuring Address Management	Not applicable	Configuration > Features > VPN > IP Address Management
	Assignment	Assignment
	Pools	IP Pools

Table A-1 Navigation Map for Configuration Tasks (continued)

VPN 3000 Task	Topic	ASDM Path
Configuring Tunneling and IPSec	PPTP	Not applicable
	IPSec site-to-site	Configuration > Features > VPN > IPSec and Configuration > Features > VPN > VPN General > Tunnel Group (and Group Policy)
	IKE proposals	Configuration > Features > VPN > IKE > Policies
	NAT-Transparency	Configuration > Features > VPN > IKE > Global Parameters (NAT Transparency group box)
	Alerts	Configuration > Features > VPN > IKE > Global Parameters
Configuring WebVPN	Not applicable	Configuration > Features > VPN > WebVPN
Configuring IP Routing	Not applicable	Configuration > Features > Routing
	Static routes	Configuration > Features > Routing > Static Route
	Default gateways (“Tunnel Default Gateway”)	Configuration > Features > Routing > Static Route
	OSPF	Configuration > Features > Routing > OSPF
	DHCP	Configuration > Features > Properties > DHCP Services
	Redundancy	Configuration > Features > Properties > Failover
	RRI	Configuration > Features > VPN > Tunnel Policy > Add > Advanced Settings > Enable Reverse Route Injection
Configuring Management Protocols	Not applicable	Not applicable
	FTP	Tools > File Transfer
	HTTP/HTTPS	Configuration > Features > Properties > HTTP/HTTPS
	TFTP	Configuration > Features > Device Administration > Administration > TFTP Server
	Telnet	Configuration > Features > Device Administration > Administration > Telnet
	SNMP	Configuration > Features > Device Administration> Administration > SNMP
	SSL	Configuration > Features > Properties > SSL
	SSH	Configuration > Features > Device Administration > Administration > Secure Shell
	XML	Not applicable

Table A-1 Navigation Map for Configuration Tasks (continued)

VPN 3000 Task	Topic	ASDM Path
Configuring Event Reporting	Event classes--list Event security levels--list Event log	Configuration > Features > Properties > Logging Event Lists Syslog Setup
	General or default handling of events FTP information for automatic backup Classes for special handling Trap destinations for SNMP management Syslog servers	Configuration > Properties > Logging > Logging Setup
	SMTP servers for email recipients	Configuration > Properties > Logging > E-Mail Setup
Configuring System Information and Parameters	Not applicable	Configuration > Features > Device Administration > Administration
	Identification	Configuration > Features > Device Administration > Administration > Device
	Time and date	Configuration > Features > Device Administration > Administration > Clock
	Sessions • Maximum active IPSec connections • Maximum active WebVPN connections	Configuration > Features > VPN > VPN General > VPN System Options
	Authentication (global parameters)	Configuration > Features > Device Administration > Administration > AAA Access
Configuring Client Update	Not applicable	Configuration > Features > VPN > VPN General > Client Update
Configuring Load Balancing	Not applicable	Configuration > Features > VPN > Load Balancing
Configuring User Management	Not applicable	Configuration > Features > Device Administration > Administration > User Accounts
	Users	Configuration > Features > Device Administration > Administration > User Accounts
	Base Group	Not applicable
	Groups	Configuration > Features > VPN > VPN General > Group Policy and Configuration > Features > VPN > VPN General > Tunnel Group

Table A-1 Navigation Map for Configuration Tasks (continued)

VPN 3000 Task	Topic	ASDM Path
Configuring Policy Management	Access hours Traffic management • Network lists • Rules • SAs • Filters • Bandwidth	Configuration > Features > Security Policy Access Rules AAA Rules Filter Rules Service Policy Rules
	NAT Policy	Configuration > Features > NAT
	Certificate group matching • Policy (for group derivation) • Rules	Configuration > Features > VPN > IKE > Certificate Group Matching • Policy • Rules
	HTTP and HTTPS	Configuration > Features > Properties > HTTP/HTTPS
	SSL	Configuration > Features > Properties > SSL
Configuring Web VPN	Not applicable	Configuration > Features > VPN > WebVPN
	Access	WebVPN Access
	Servers and URLs	Servers and URLs
	Port Forwarding	Port Forwarding
	Home Page	Homepage
	Proxies	Proxies
	AAA	WebVPN AAA
	NetBios Servers	NetBIOS Servers
	ACLs	ACLs

Table A-2 Navigation Map for Administration Tasks

VPN 3000 Task	Topic	ASDM Path
Viewing statistics for all active sessions	Not applicable	Monitoring > Features > VPN and Monitoring > Features Administration
	Updating the display	Click **Refresh**
Updating the ASA system software	Not applicable	Tools > Upload Image From Local PC
Updating the VPN Client software	Not applicable	Configuration > Features > VPN > VPN General > Client Update
Shutting down and/or rebooting the system	Not applicable	Tools > System Reload
Viewing the reboot status	Not applicable	Tools > System Reload
Using the Ping utility	Not applicable	Tools > Ping

Table A-2 Navigation Map for Administration Tasks (continued)

VPN 3000 Task	Topic	ASDM Path
Configuring and controlling administrative access rights	Configure administrator usernames, access, and rights Configure ACLs for administrators Configure access settings	Configuration > Features > Device Administration > Administration > AAA Access
	Configure AAA servers for admin users	Configuration > Features > Properties > AAA Setup > AAA Servers
	Managing files in flash memory on the device	Tools > File Management
	Swap backup and boot configuration files	Tools > Upload Image from Local PC
	Transfer files using TFTP	Tools > File Transfer > TFTP
	Send a file using HTTP	Tools > File Transfer > HTTP
	Export the configuration to an XML file	Not applicable
Enrolling for and Managing Certificates (PKI)	Enrolling for a certificate Obtaining an SSL certificate Enabling CRL checking and caching Enabling digital certificates for remote access connections Enabling digital certificates for site-to-site connections Deleting digital certificates Managing certificates • Enrolling identity and SSL certificates • Installing certificates once enrolled Configuring SCEP parameters Viewing CRL cache Viewing certificate information Configuring a CA certificate Renewing a certificate Managing enrollment requests	Configuration > Features > Device Administration > Certificate Keypair Trustpoint Authentication Enrollment Import Certificate Manage Certificate

Table A-3 Monitoring Tasks

VPN 3000 Task	Topic	ASDM Path
Monitoring the routing table (routes and protocols)	Not applicable	Monitoring > Features > Routing > Routes Monitoring > Features > Routing > OSPF LSAs Monitoring > Features > Routing > OSPF Neighbors
Viewing dynamic filters and rules	Not applicable	Configuration > Features > Security Policy
Viewing the event log	Not applicable	Monitoring > Features > Logging > Live Log
Viewing system status and memory status	Not applicable	Monitoring > Features > Administration > System Graphs
Displaying information about all active sessions	Not applicable	Monitoring > Features > VPN > VPN Statistics > Sessions Monitoring > Features > VPN > VPN Statistics > L2TP Sessions
Gathering Statistics	Not applicable	Monitoring > Features
	Accounting	Monitoring > Features > Administration > AAA Servers
	Address pools	
	Administrative AAA	Monitoring > Features > Administration > AAA Servers
	Authentication	Monitoring > Features > Administration > Authenticated Users
	Authorization	Monitoring > Features > Administration > AAA Servers
	Bandwidth management	Monitoring > Features > Administration > System Graphs
	Compression	Not applicable
	DHCP	Monitoring > Features > Interfaces > DHCP
	DNS	Monitoring > Features > Administration > DNS Cache
	Events	Monitoring > Features > Logging > Live Log
	Filtering	Not applicable
	HTTP IPSec L2TP Load balancing NAT	Monitoring > Features > VPN > VPN Statistics > Protocol Statistics
	PPTP	Not applicable
	SSH	Monitoring > Features > Administration > Secure Shell Sessions
	SSL	Monitoring > Features > Administration > ASDM > HTTPS Sessions
	Telnet	Monitoring > Features > Administration > Telnet Sessions
	VRRP	Not applicable

Mapping Debug/Event Levels from VPN 3000 Series Concentrators to the ASA

The VPN 3000 Series Concentrator has 13 logging severity levels, while the ASA uses the numbers from 1 through 11, then 254 and 255 to represent different levels of debugging. In both systems, lower numbers indicate greater severity; for example, selecting a severity level of 3 in either system displays only event messages of the three greatest severity levels. Table B-1 shows the mapping between the VPN 3000 Concentrator severity levels and the ASA severity levels.

Table B-1 Debug Level Map

VPN 3000 Debug Level	ASA Debug Level
1, 2, 3	1
4	2
5	3
6	4
7	5
8	6
9	7
10	8
11	9
12	10
13	11, 254, 255

The ASA debug levels 254 and 255 have special meanings.

- 254 specifies IKE packet decode. This displays a Sniffer-like decoding of fields and values for each IKE packet.
- 255 specifies an IKE packet dump, which displays the octets within the packets.

Selecting higher-numbered levels results in the display of greater amounts of data, because the capture includes logging messages for that level and for all lower-numbered (that is, more severe) levels.

If you select level 254 or 255, the debug trace queue might overflow. To avoid this overflow, use the **capture** command, specifying a name for the area in memory that will hold the information and the name of the interface on which to apply packet capture, as follows:

```
hostname(config)# capture name type isakmp interface interface-name
```

This command stores the data to an area in memory, which you can then display or write to a file, then post-process to extract the information. See the description of the **capture** command for more information on its use.

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W