Selected ASDM VPN Procedures, Version 5.2(1)

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: N/A, Online only
Text Part Number: OL-10670-01

Selected ASDM VPN Procedures, Version 5.2(1)

About This Guide

This guide explains how to use ASDM to configure selected VPN features on the Adaptive Security Appliance.

Audience

This guide is for system engineers (SEs) and network administrators who use the Adaptive Security Device Manager to set up and configure ASAs for virtual private networking. You should be familiar with networking equipment, basic networking concepts and virtual private networking.

Organization

The following table describes each chapter in this guide:

Chapter	Description
Chapter 1, “Enrolling for Digital Certificates”	Provides information on enrolling for digital certificates, generating key pairs, creating a trustpoint, and using SCEP to obtain certificates.
Chapter 2, “Configuring Group Policies”	Provides information on configuring group policies. Describes how group policies relate to tunnel groups and users.
Chapter 3, “Configuring the SSL VPN Client”	Provides information on configuring SVC, which is a VPN tunneling technology that gives remote users the benefits of an IPSec VPN client without the need for network administrators to install and configure IPSec VPN clients on remote computers.
Chapter 4, “Configuring Client Update for Windows and VPN 3002 Clients”	Describes how to configure client update, which lets administrators at a central location automatically notify VPN client users that it is time to update VPN client software and the VPN 3002 hardware client image.
Chapter 5, “Configuring DDNS Updates”	Describes how to configure the DHCP server to update dynamic DNS resource records.

Chapter	Description
Chapter 6, "Configuring an LDAP AAA Server"	Presents an example configuration procedure for configuring security appliance user authentication and authorization using a Microsoft Active Directory Server (LDAP) that sits on the same internal network as the security appliance.
Chapter 7, "Configuring Citrix MetaFrame Services"	Provides information about configuring the security appliance to support Citrix MetaFrame services. Includes instructions on configuring certificates for this purpose.
Chapter 8, "Configuring Single Sign-on for WebVPN"	Provides information about SSO, which lets WebVPN users enter a username and password only once to access multiple protected services and web servers. Includes instructions for configuring Siteminder SSO and HTTP Form protocol.
Chapter 9, "Configuring Network Admission Control"	Provides information on configuring Network Admission Control, which protects the enterprise network from intrusion and infection from worms, viruses, and rogue applications by performing endpoint compliancy and vulnerability checks as a condition for production access to the network.
Chapter 10, "Configuring L2TP over IPSec"	Describes how to configure the security appliance to let remote Windows clients use Layer 2 Tunneling Protocol (L2TP) to access the public IP network to securely communicate with private corporate network servers.
Chapter 11, "Configuring Load Balancing"	Describes the concept of load balancing and how to configure load balancing on an ASA model 5520 or higher.
Chapter 12, "Configuring Easy VPN Services on the ASA 5505"	Describes how to configure an VPN services on an ASA 5505, which can run as a hardware client or as a headend, but not both at the same time.

Related Documentation

This guide is a companion to the following user guides:

- *Cisco ASA 5500 Series Release Notes*
- *Cisco ASDM Release Notes*
- *Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series*
- *Cisco ASA 5500 Series Hardware Installation Guide*
- *Cisco ASA 5500 Series Quick Start Guide*
- *Cisco Security Appliance Command Line Configuration Guide*
- *Cisco Security Appliance Command Reference*
- *Migrating to ASA 7.1(1) from the VPN 3000 Series Concentrator*

- *Release Notes for Cisco Secure Desktop*
- *Cisco Security Appliance Logging Configuration and System Log Message*s

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.

Type of Data	Format
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

Enrolling for Digital Certificates

This chapter describes how to enroll for a digital certificate using 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 chapter.

This chapter includes the following sections:

Note As you following the instructions in this chapter, click **Help** for more information about the attributes shown in the ASDM windows.

Overview of Configuration Procedure

To enroll with a CA and get an identity certificate for authenticating tunnels, complete the following tasks.

Note This example shows automatic (SCEP) enrollment.

1. Create a key pair for the identity certificate. The key pair are 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.

Understanding 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 are RSA keys.

- The maximum key modulus is 2048 The default size is 1024 bits.
- For signature operations, the maximum key size is 4096 bits.
- 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.

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 specified label using ASDM, and use the default settings for the other parameters.

Generating an RSA Key Pair

To generate an RSA key pair, perform the following steps.

Step 1 In the **Configuration > Properties > Certificate > Key Pair** window, 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 default RSA key, but you could, instead, enter a name such as key1.

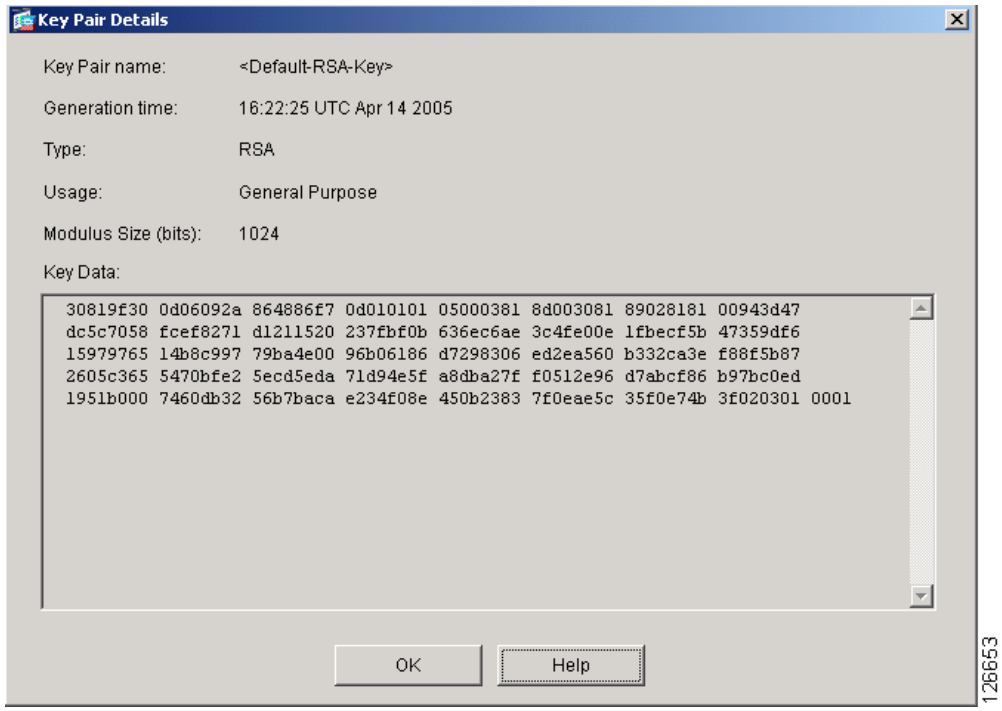
b. **Size** list—For an RSA key pair, the **Size** list displays the options: 512, 768, 1024, or 2048. The default size is 1024. This example accepts the default setting.

c. **Usage** options— 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 1-1 shows sample output.

Figure 1-1 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.

To create a trustpoint, perform the following steps.

Step 1 In the **Configuration > Properties > Certificate > Trustpoint > Configuration** window, 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** field—Type the trustpoint name in the **Trustpoint Name** field. For this example, the name is newmsroot.

b. **Enrollment URL** field—In the **Enrollment Settings** window, under the **Enrollment Mode** area, click the **Use automatic enrollment** option. Then type the enrollment URL in the field. 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** window, select the key pair you configured for this trustpoint in the **Key Pair** list. For this example, the key pair is key1.

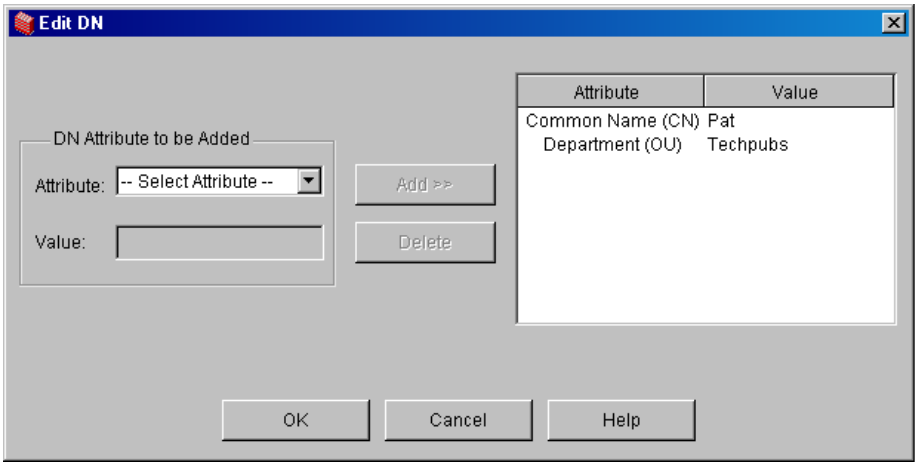
b. In the **Enrollment Settings** window, click **Certificate Parameters**.

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

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

For this example, first select **Common Name (CN)**, type **Pat** in the **Value** field, and click Add; then select **Department (OU)** and type **Techpubs** in the **Value** field. Figure 1-2 shows what you have entered in the **Edit DN** dialog box.

Figure 1-2 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

This section shows 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 security appliance 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 security appliance prompts you to paste the base-64 formatted CA certificate into the text box.

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.

To obtain certificates, perform the following steps.

Step 1 Select the **Configuration > Properties > Certificate > Authentication** window.

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 by performing the following steps.

Step 1 In the **Configuration > Properties > Certificate > Enrollment** window, select the trustpoint in the **Trustpoint Name** list. For this example, you would select **newmsroot**.

Step 2 Click **Enroll**.

Managing Certificates

To manage certificates, use the **Configuration > Properties > Certificate > Manage Certificates** window.

You can use this window to add a new certificate and delete a certificate.

This pane displays the following information:

- Subject—Identifies the owner of the certificate.
- Type—CA, RA general, RA encryption, RA signature, identity.
- 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 yet issued the identity certificate.
- Usage—identifies how the certificate is used: signature, general purpose, or encryption.

You can also display information about a certificate by clicking **Show Details**. The Certificate Details dialog displays three tables: General, Subject, and Issuer.

General—Displays the values for type, serial number, status, usage, CRL distribution point, the time within which the certificate is valid, and associated trustpoints. This applies to both available and pending status.

Subject— Displays the X.500 fields of the subject DN or certificate owner and their values. This applies only to available status.

Issuer—Displays the X.500 fields of the entity that granted the certificate. This applies only to available status.

Configuring Group Policies

This chapter describes how to configure VPN group policies using ASDM. This chapter includes the following sections.

Groups, group policies, tunnel groups, and users, are interdependent. In summary, you first configure tunnel groups to set the values for the connection. Then you configure group policies. These set values for users in the aggregate. Then you configure users, which can inherit values from groups and configure certain values on an individual user basis. This chapter describes how and why to configure group policies.

Overview of Group Policies, Tunnel Groups, and Users

Although this chapter deals only with group policies, you should understand the context in which these group policies exist. Groups and users are core concepts in managing the security of virtual private networks (VPNs) and in configuring the security appliance. They specify attributes that determine user access to and use of the VPN. A *group* is a collection of users treated as a single entity. *Users* get their attributes from *group policies*. *Tunnel groups* identify the group policy for a specific connection. If you do not assign a particular group policy to a user, the default group policy for the connection applies.

Tunnel groups and group policies simplify system management. To streamline the configuration task, the security appliance provides a default LAN-to-LAN tunnel group, a default remote access tunnel group, a default WebVPN tunnel group, and a default group policy (DfltGrpPolicy). The default tunnel groups and group policy provide settings that are likely to be common for many users. As you add users, you can specify that they “inherit” parameters from a group policy. Thus, you can quickly configure VPN access for large numbers of users.

If you decide to grant identical rights to all VPN users, then you do not need to configure specific tunnel groups or group policies, but VPNs seldom work that way. For example, you might allow a finance group to access one part of a private network, a customer support group to access another part, and an MIS group to access other parts. In addition, you might allow specific users within MIS to access systems that other MIS users cannot access. Tunnel groups and group policies provide the flexibility to do so securely.

Note The security appliance 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. For more information about using object groups, see *Cisco Security Appliance Command Line Configuration Guide*, Chapter 16, "Identifying Traffic with Access Lists."

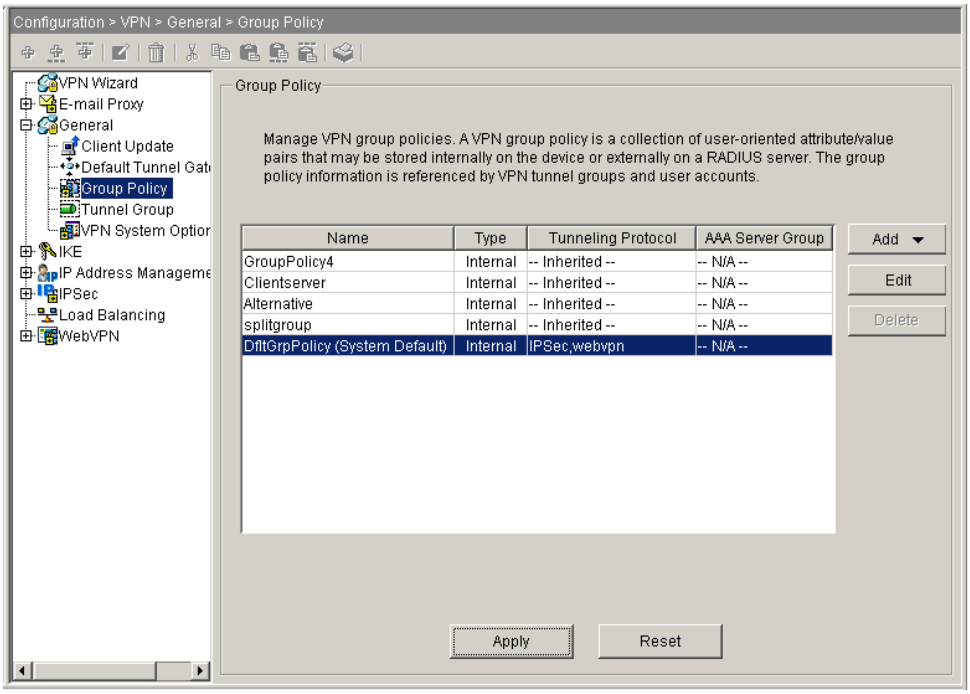
Group Policies

Group policies let you apply whole sets of attributes to a user or a group of users, rather than having to specify each attribute individually for each user. You can also modify the group-policy attributes for a specific user.

A group policy is a set of user-oriented attribute/value pairs for IPSec connections that are stored either internally (locally) on the device or externally on a RADIUS or LDAP server. A tunnel group uses a group policy that sets terms for user connections after the tunnel is established.

To assign a group policy to users or to modify a group policy for specific users, select **Configuration > VPN > General > Group Policy** (Figure 2-1).

Figure 2-1 Group Policy Window



You can configure internal and external group policies. Internal groups are configured on the security appliance internal database. External groups are configured on an external authentication server, such as RADIUS or LDAP. Group policies include the following attributes:

- Identity
- Server definitions

- Client firewall settings
- Tunneling protocols
- IPSec settings
- Hardware client settings
- Filters
- Client configuration settings
- Network Admission Control settings
- WebVPN functions
- Connection settings

Default Group Policy

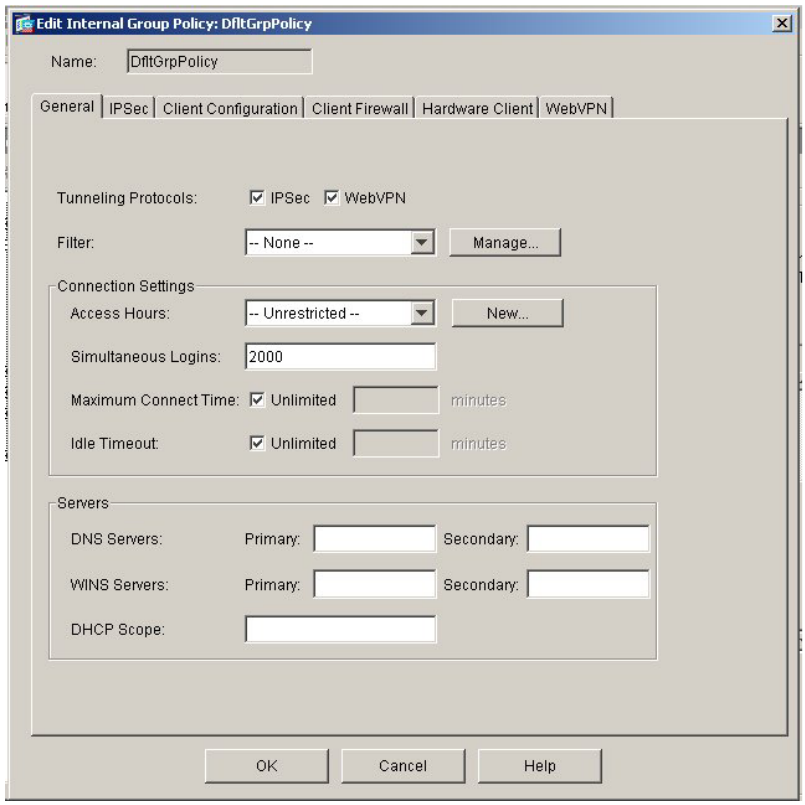
The security appliance supplies a default group policy, named DfltGrpPolicy, which always exists on the security appliance. This default group policy does not take effect unless you configure the security appliance to use it. DfltGrpPolicy is always an internal group policy. You can modify this default group policy, but you cannot delete it. When you configure other group policies, any attribute that you do not explicitly specify takes its value from the default group policy.

The Group Policy window lets you manage VPN group policies. Configuring the default VPN group policy lets users inherit attributes that you have not configured at the individual group or username level. By default, VPN users have no group policy association. The group policy information is used by VPN tunnel groups and user accounts.

The “child” windows, tabs, and dialog boxes let you configure the default group parameters. These parameters are those that are most likely to be common across all groups and users, and they streamline the configuration task. Groups can “inherit” parameters from this default group, and users can “inherit” parameters from their group or the default group. You can override these parameters as you configure groups and users.

To modify the default group policy, select DfltGrpPolicy in the table on the Group Policy window and click **Edit**. The Edit Internal Group Policy: DfltGrpPolicy window appears (Figure 2-2):

Figure 2-2 Edit Internal Group Policy: DfltGrpPolicy Window



To change any of the attributes of the default group policy, work through the selections on the various tabs on the Edit Internal Group Policy: DfltGrpPolicy window, just as you would for any other internal group policy, as described in Configuring an Internal Group Policy, page 2-9.

The default group policy, DfltGrpPolicy, that the security appliance has the following attributes:

```
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
 wins-server none
 dns-server none
 vpn-access-hours none
 vpn-simultaneous-logins 3
 vpn-idle-timeout 30
 vpn-session-timeout none
 vpn-filter none
 vpn-tunnel-protocol IPSec
 password-storage disable
 ip-comp disable
 re-xauth disable
 group-lock none
 pfs disable
 banner none
 ipsec-udp disable
 ipsec-udp-port 10000
 split-tunnel-policy tunnelall
 split-tunnel-network-list none
 default-domain none
 split-dns none
 secure-unit-authentication disable
```

```
user-authentication disable
user-authentication-idle-timeout 30
ip-phone-bypass disable
leap-bypass disable
nem disable
backup-servers keep-client-config
client-firewall none
client-access-rule none
webvpn
 functions url-entry
 no html-content-filter
 no homepage
 no filter
 no url-list
 no port-forward
 port-forward-name value Application Access
```

Configuring Group Policies

This section includes the following sections:

A group policy can apply to any kind of tunnel. In each case, if you do not explicitly define a parameter, the group takes the value from the default group policy. To configure (add or modify) a group policy, follow the steps in the subsequent sections.

If you click the Add dialog box, a small menu appears giving you the option to create a new internal group policy, or an external group policy that is stored externally on a RADIUS or LDAP server. Both the Add Internal Group Policy window and the Edit Group Policy window include tabbed sections. If you click the WebVPN tab, you expose several additional tabs. Click each tab to display its parameters. As you move from tab to tab, the security appliance retains your settings. When you have finished setting parameters on all tabbed sections, click OK or Cancel.

In these dialog boxes, you configure the following kinds of parameters:

- General Parameters: Protocols, filtering, connection settings, and servers.
- IPSec Parameters: IP Security tunneling protocol parameters and client access rules.
- Client Configuration Parameters: Banner, password storage, split-tunneling policy, default domain name, IPSec over UDP, backup servers.
- Client FW Parameters: VPN Client personal firewall requirements.
- Hardware Client Parameters: Interactive hardware client and individual user authentication; network extension mode.

- Network Admission Control parameters.
- WebVPN Parameters: SSL VPN access.

Before configuring these parameters, you should configure:

- Access hours.
- Rules and filters.
- IPSec Security Associations.
- Network lists for filtering and split tunneling
- User authentication servers, and specifically the internal authentication server.

Configuring an External Group Policy

External group policies take their attribute values from the external server that you specify. For an external group policy, you must identify the AAA server group that the security appliance can query for attributes and specify the password to use when retrieving attributes from the external AAA server group. If you are using an external authentication server, and if your external group-policy attributes exist in the same RADIUS server as the users that you plan to authenticate, you have to make sure that there is no name duplication between them.

Note External group names on the security appliance refer to user names on the RADIUS server. In other words, if you configure external group X on the security appliance, the RADIUS server sees the query as an authentication request for user X. So external groups are really just user accounts on the RADIUS server that have special meaning to the security appliance. If your external group attributes exist in the same RADIUS server as the users that you plan to authenticate, there must be no name duplication between them.

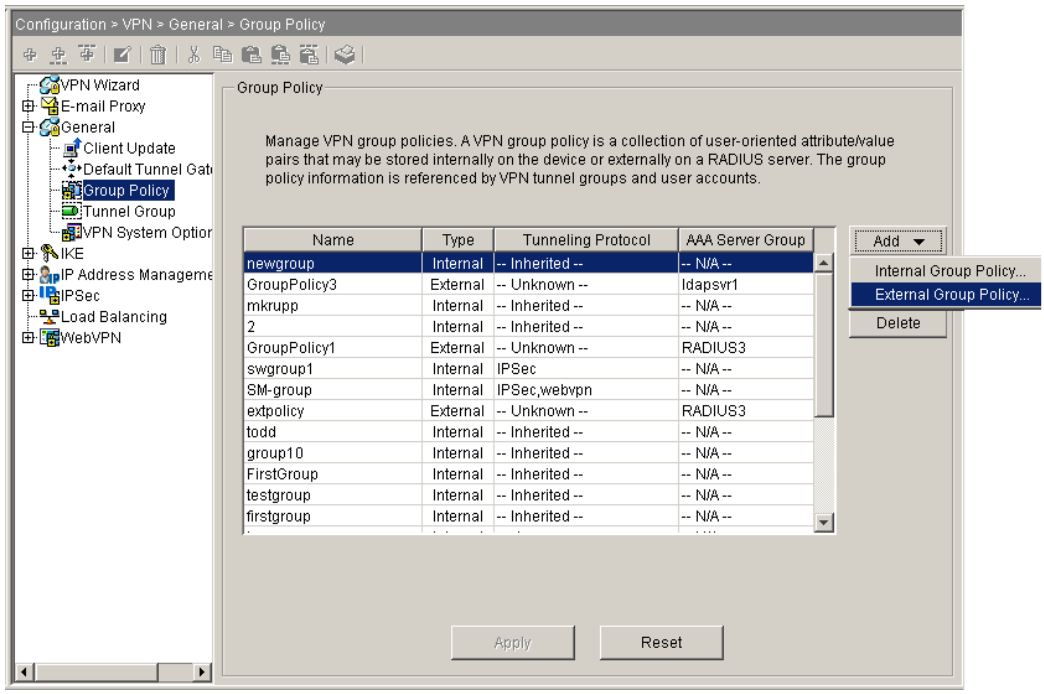
The security appliance supports user authorization on an external LDAP or RADIUS server. Before you configure the security appliance to use an external server, you must configure the server with the correct security appliance authorization attributes and, from a subset of these attributes, assign specific permissions to individual users. Follow the instructions in the *Cisco Security Appliance Command Line Configuration Guide*, Appendix E, "Configuring an External Server for Security Appliance User Authorization" to configure your external server.

Adding an External Group Policy

The following steps explain how to add an external group policy.

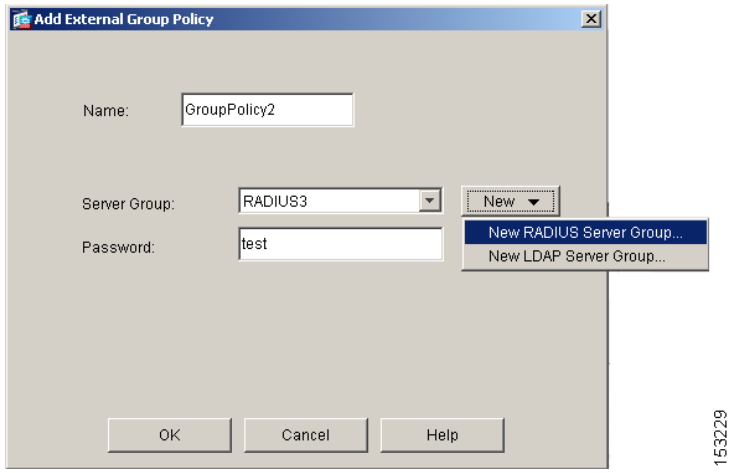
Step 1 To add an external group policy, select **Configuration > VPN > General > Group Policy**, click **Add**, and select **External Group Policy** from the menu (Figure 2-3).

Figure 2-3 Adding an External Group Policy



The Add External Group Policy dialog box appears (Figure 2-4).

Figure 2-4 Add External Group Policy Dialog Box

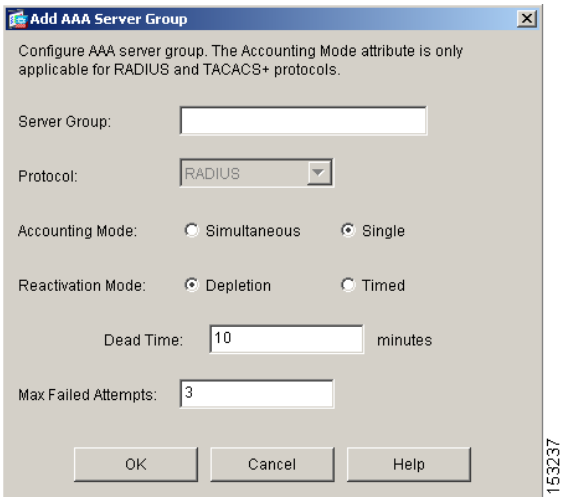


To configure the attributes of the new external group policy, do the following steps, specifying a name and type for the group policy, along with the server-group name and a password.

Step 2 Enter a name for the group policy and a password for the server. Then select a server group from the list or click New to create a new server group. When you click New, a menu appears. Select either a new RADIUS server group or a new LDAP server group. Either of these options opens the Add AAA Server Group dialog box (Figure 2-5). Click OK when done.

Note For an external group policy, RADIUS is the only supported AAA server type.

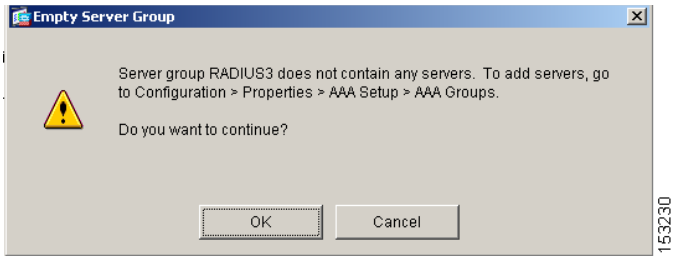
Figure 2-5 Add AAA Server Group Dialog Box



Step 3 Configure the AAA server group parameters. The Add AAA Server Group dialog box lets you configure a new AAA server group with the following attributes. The Accounting Mode attribute applies only to RADIUS and TACACS+ protocols.

- Server Group—Specifies the name of the server group. You can specify the name of a new server group, then add servers to that group. If the server group name that you specify does not contain any servers, you see the following message (Figure 2-6):

Figure 2-6 Empty Server Group Message



To add servers to a group, select **Configuration > Properties >AAA Setup > AAA Groups**. To continue after seeing this message, click **OK**. To exit the external group configuration procedure, click **Cancel**.

- Protocol—(*Display only*) Indicates whether this is a RADIUS or an LDAP server group. For an external group policy, this is always RADIUS.
- Accounting Mode—(*RADIUS and TACACS+ protocols only*) Indicates whether to use simultaneous or single accounting mode. In single mode, the security appliance sends accounting data to only one server. In simultaneous mode, the security appliance sends accounting data to all servers in the group.

- Reactivation Mode—Specifies the method by which failed servers are reactivated: Depletion or Timed reactivation mode. In Depletion mode, failed servers are reactivated only after all of the servers in the group become inactive. In Timed mode, failed servers are reactivated after 30 seconds of down time.
- Dead Time—Specifies, for depletion mode, the number of minutes that must elapse between the disabling of the last server in the group and the subsequent re-enabling of all servers. This field is not available for timed mode.
- Max Failed Attempts— Specifies the number (an integer in the range 1 through 5) of failed connection attempts allowed before declaring a nonresponsive server inactive.

Note You can configure several vendor-specific attributes (VSAs), as described in *Cisco Security Appliance Command Line Configuration Guide* Appendix E, "Configuring an External Server for Security Appliance User Authorization". If a RADIUS server is configured to return the Class attribute (#25), the security appliance uses that attribute to authenticate the Group Name. On the RADIUS server, the attribute must be formatted as: OU=*groupname*; where *groupname* is identical to the Group Name configured on the security appliance—for example, OU=Finance.

Editing an External Group Policy

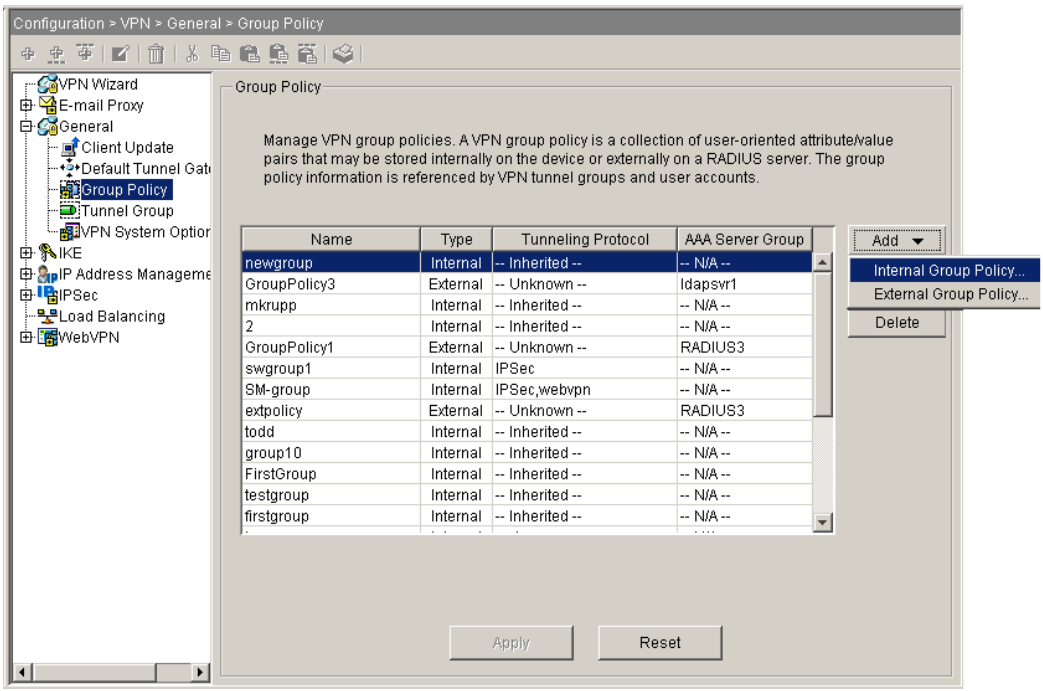
The procedures for editing a group policy are similar to those for adding, except that when you click **Edit** on the Group Policy window, the Edit Group Policy window appears, with the Name field already filled in. The rest of the fields on this window are the same. You can also add a AAA server group when you edit an external group policy. See Steps 2 and 3 of Adding an External Group Policy, page 2-6.

Configuring an Internal Group Policy

Internal group policies are configured on the security appliance internal database. To configure the attributes of the new internal group policy, do the following steps.

Step 1 To add or edit an internal group policy, select **Configuration >VPN > General >Group Policy**. The Group Policy window appears (Figure 2-7).

Figure 2-7 Group Policy Window, Add Internal Group Policy

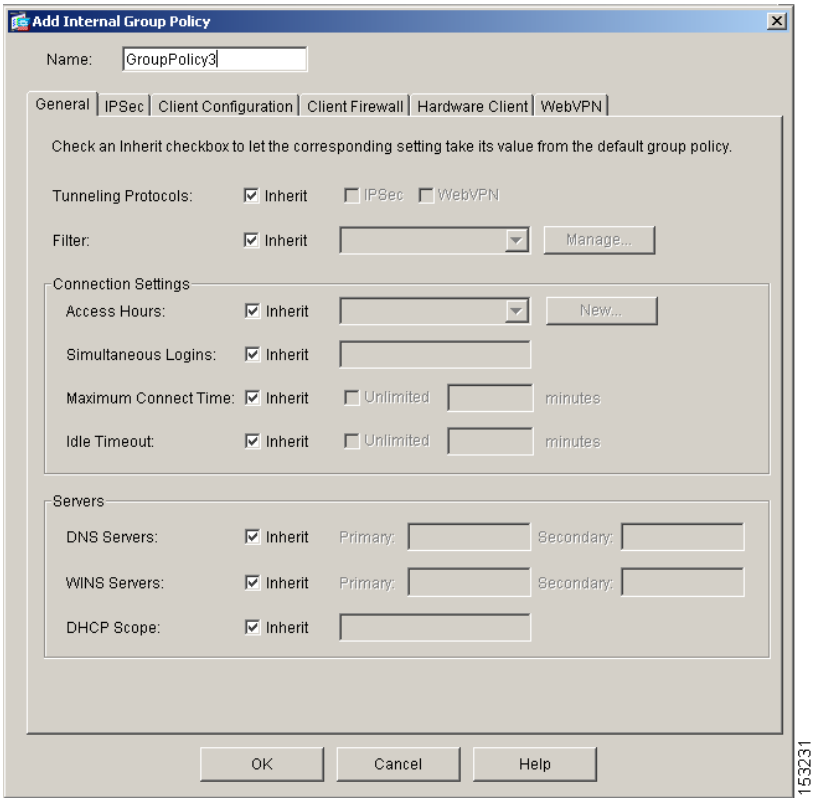


Step 2 Click **Add** or **Edit**.

- If you are adding an internal group policy, select **Internal Group Policy** from the menu. The Add Internal Group Policy window appears (Figure 2-8).
- If you are editing an internal group policy, the Edit Internal Group Policy window appears.

The contents of these windows are similar, the only difference being that for editing, the Name field is display-only. Because of this similarity, the following procedures show only the Add Internal Group Policy window.

Figure 2-8 Add Internal Group Policy Window



This window offers several tabs, on which you configure function-specific attributes. In most cases, you can check the Inherit check box to take the corresponding setting from the default group policy. Allowing inheritance can greatly simplify the configuration process. You can explicitly configure those attributes that you do not want to be inherited. The following sections explain how to configure the group policy attributes for an internal group policy.

Configuring Internal Group Policy General Attributes

The Add or Edit Internal Group Policy window, General tab lets you configure tunneling protocols, ACL filters, connection settings, and servers for the group policy being added or modified. For each of the fields on this window, checking the Inherit check box lets the corresponding setting take its value from the default group policy. Clearing the Inherit check box lets you configure specific values.

The following sections explain how to configure the values of each of the attributes in the General tab.

Configuring Tunneling Protocols

Select the tunneling protocol or protocols that this group can use. Users can use only the selected protocols. You must configure at least one tunneling mode for users to connect over a VPN tunnel. The default is IPSec.

The choices are as follows:

- IPSec—IP Security Protocol. Regarded as the most secure protocol, IPSec provides the most complete architecture for VPN tunnels. Both LAN-to-LAN (peer-to-peer) connections and client-to-LAN connections can use IPSec. When you check the IPSec check box, the security appliance negotiates an IPSec tunnel between two peers (a remote access client or another secure gateway) and creates security associations that govern authentication, encryption, encapsulation, and key management.
- WebVPN—VPN via SSL/TLS. Checking the WebVPN check box provides VPN services to remote users via an HTTPS-enabled web browser and does not require a client (either hardware or software). This protocol uses a web browser to establish a secure remote-access tunnel to a security appliance. WebVPN can provide easy access to a broad range of enterprise resources, including corporate websites, web-enabled applications, NT/AD file share (web-enabled), e-mail, and other TCP-based applications from almost any computer that can reach HTTPS Internet sites.
- L2TP over IPSec—Allows remote users with VPN clients provided with several common PC and mobile PC operating systems to establish secure connections over the public IP network to the security appliance and private corporate networks. L2TP uses PPP over UDP (port 1701) to tunnel the data. The security appliance must be configured for IPSec transport mode.

Note If no protocol is selected, an error message appears.

To remove a protocol attribute from the running configuration, clear the check box for that protocol.

Configuring the ACL Filter

Filters consist of 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. You configure ACLs to permit or deny various types of traffic for this group policy. (You can also configure this attribute in username mode, in which case the value configured under username supersedes the group-policy value.)

Note The security appliance supports only an inbound ACL on an interface.

At the end of each ACL, there is an implicit, unwritten rule that denies all traffic that is not explicitly permitted by an access control entry (ACE). ACEs are referred to as rules in this topic.

To specify that you want the group policy to inherit the filter from the default group policy, click the Inherit check box. This is the default value. To specify a different filter, select a filter from the menu. To prevent inheriting a value, select **None** instead of specifying an ACL name. The **None** option indicates that there is no access list and sets a null value, thereby disallowing an access list.

Note You might not know at configuration time what values the group policy is inheriting. To ensure that no ACL is associated with a particular group policy, clear the Inherit check box and select **None** in the ACL (Filter/Web-VPN ACL ID/...) drop-down list.

If you are dealing with one of the default group policies, inheritance is inapplicable, so only selecting **None** is relevant.

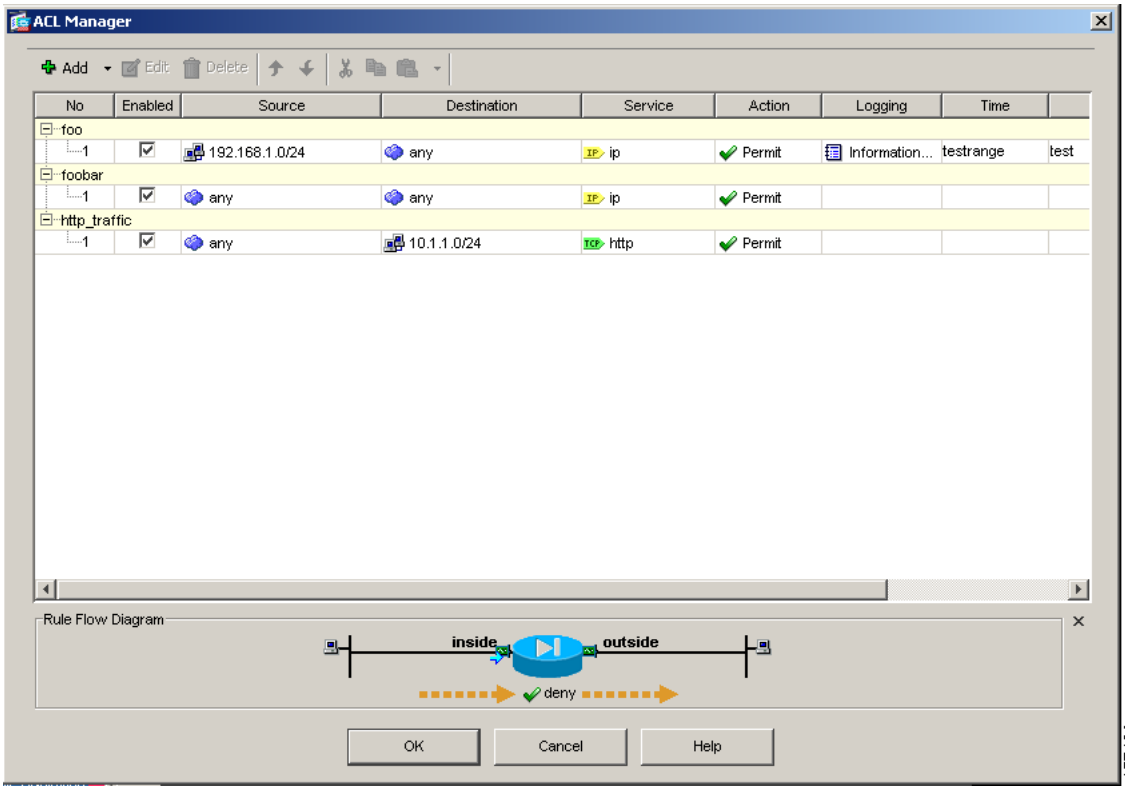
If you select Inherit or None, you do not add or modify an existing filter, so you can skip to Configuring Access Hours, page 2-24 in these instructions.

Managing ACLs and ACEs

To create a new filter (ACL) or modify an existing filter, click **Manage**. The ACL Manager dialog box (Figure 2-9) appears. In this dialog box, you can add, edit, and delete Access Control Lists (ACLs) and Extended Access Control Lists (ACEs) to control the access of a specific host or network to another host/network, including the protocol or port that can be used.

To remove an ACL from the group policy, select **Delete** from the toolbar. There is no confirmation or undo.

Figure 2-9 ACL Manager Dialog Box



The fields in this dialog box are as follows:

- No—Indicates the order of evaluation for the rule. Implicit rules are not numbered, but are represented by a hyphen.
- Enabled—Enables or disables a rule. Implicit rules cannot be disabled.
- Source—Shows the IP addresses of the hosts/networks that are permitted or denied to send traffic to the IP addresses listed in the Destination column. An address column might contain an interface name with the word any, such as inside: any. This means that any host on the inside interface is affected by the rule.
- Destination—Shows the IP addresses of the hosts/networks that are permitted or denied to receive traffic from the IP addresses listed in the Source Host/Network column. An address column might contain an interface name with the word any, such as outside: any. This means that any host on the outside interface is affected by the rule. An address column might also contain IP addresses in square brackets; for example [209.165.201.1-209.165.201.30]. These addresses are translated addresses. When an inside host makes a connection to an outside host, the firewall maps the address

of the inside host to an address from the pool. After a host creates an outbound connection, the firewall maintains this address mapping. The address mapping structure is called an xlate, and remains in memory for a period of time. During this time, outside hosts can initiate connections to the inside host using the translated address from the pool, if allowed by the ACL. Normally, outside-to-inside connections require a static translation so that the inside host always uses the same IP address.

- Service—Names the service and protocol specified by the rule. See Managing Protocol and Service Groups, page 2-17 for more information about protocols and services.
- Action—Shows the action that applies to the rule, either Permit or Deny.
- Logging—Shows the logging level and the interval in seconds between log messages (if you enable logging for the ACL). To set logging options, including enabling and disabling logging, choose **Edit** from the toolbar. The Edit ACE dialog box appears. This dialog box is identical to the Add ACE dialog box (Figure 2-12), except for the title bar.
- Time—Shows the name of the time range to be applied in this rule. The time range specifies the access hours during which the user can connect using this group policy. The default value is (any), meaning that there is no restriction on when the user can connect.
- Description—Shows the description you typed when you added the rule. An implicit rule includes the following description: "Implicit outbound rule." To edit the description, choose **Edit** from the toolbar. The Edit ACE dialog box appears. This dialog box is identical to the Add ACE dialog box (Figure 2-12), except for the title bar.
- Rule Flow Diagram—(Read-only) Shows a graphic representation of the selected rule flow. To close this diagram, click the small "X" at the top of the Rule Flow Diagram area.This same diagram appears on the ACL Manager dialog box unless you explicitly close that display.

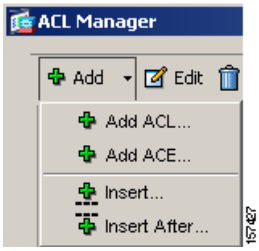
Rules are applied in the order in which they appear in the table in the ACL Manager dialog box. To move a rule up or down in the list, click the up or down arrows on the toolbar. To delete a rule, select it, then click **Delete**.

You can also cut, copy, and paste ACLs and ACEs, just as you would in a text document, by clicking the scissors (cut), pages (copy), and clipboard (paste) icons on the toolbar.

Double-clicking on any row of the ACL Manager table opens the Edit ACL dialog box, where you can modify these fields.

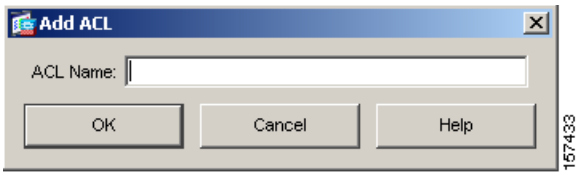
To add a new ACL, click **Add** and select **Add ACL** from the drop-down list (Figure 2-10).

Figure 2-10 Add/Insert Menu



The Add ACL dialog box appears (Figure 2-11). Enter an ACL name and click OK.

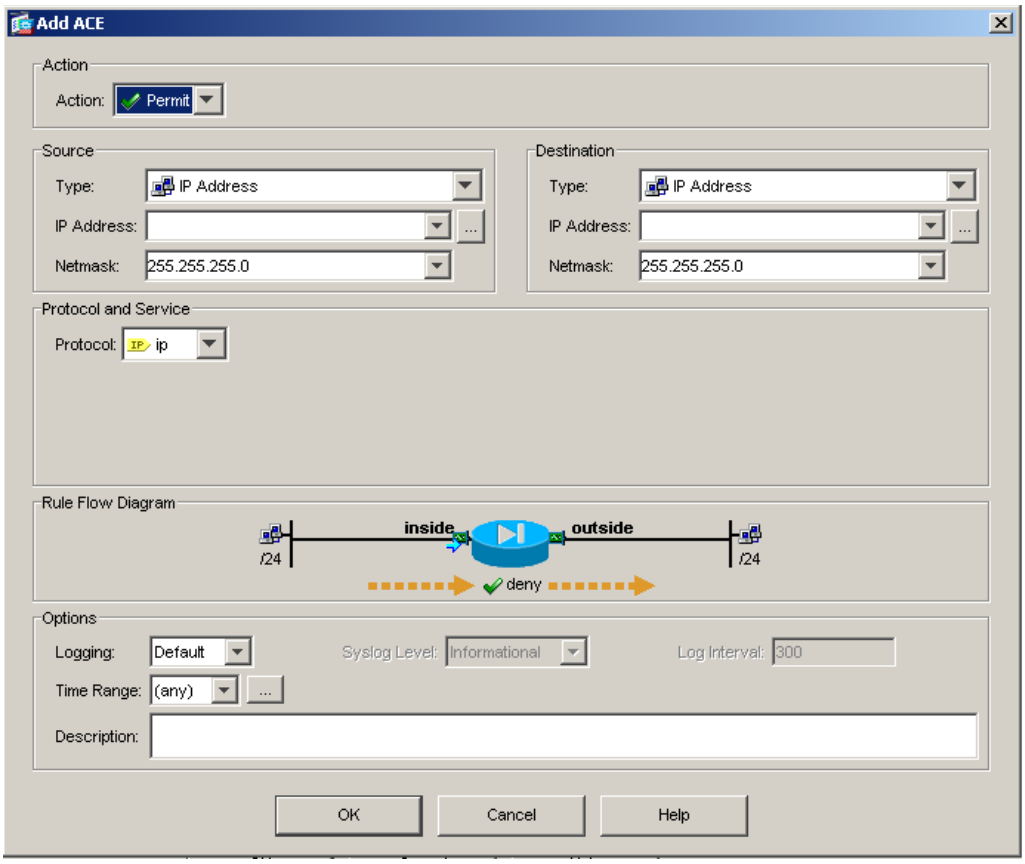
Figure 2-11 Add ACL Dialog Box



After you add an ACL, you can populate it with filter rules using the **Add ACE** menu selection.

To add a filter rule, click **Add ACE** (Figure 2-10). To edit a filter rule, select the rule you want to change and click **Edit**. The Add or Edit Extended Access List Rule dialog box appears (Figure 2-12). The Edit Extended Access List Rule dialog box is identical with the Add ACE dialog box, except for the title.

Figure 2-12 Add ACE



This dialog box lets you configure whether to permit or deny traffic, specify the source and destination host or network, specify the protocol, service (source and destination ports) to which to apply this rule, specify a time range to apply or define a new time range, configure the syslog options, and manage the service groups. Optionally, you can also enter a description of this rule. Your entries here appear in the Rule Flow Diagram and in the Configure ACLs table in the ACL Manager dialog box.

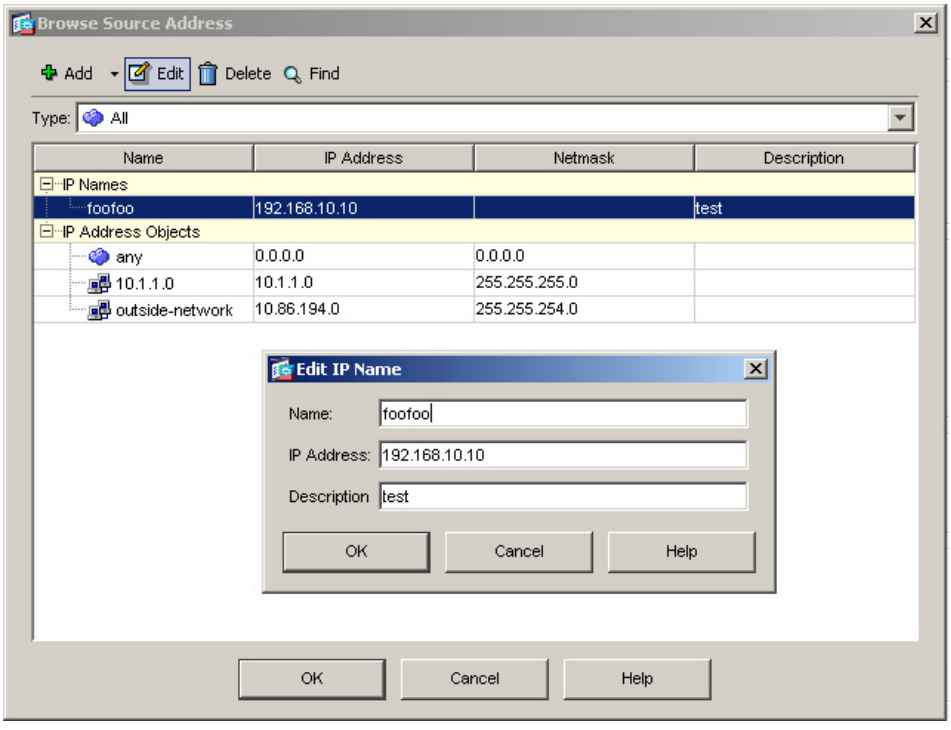
Note The contents of the Source, Destination, Protocol and Service, Rule Flow Diagram, and Options areas on this dialog box change, depending on your selections.

Configuring the Source and Destination Areas

Use these areas to identify the source and destination networks. Specify the following parameters for both the source and destination areas:

- Type—Select the type of the source or destination address to which this rule applies. You can identify the networks by IP address, interface IP, or network object group. You can also select the keyword **any** to specify that this rule applies to any source or destination. The any type has no additional qualifying fields for source or destination.
  - IP address and Netmask—When you select IP Address in the Type field, use the IP address field to specify the IP address of the source or destination network or host and the Netmask field to select the subnet mask for the specified IP address. For example, the address/netmask 192.168.10.0/255.255.255.0 specifies a network, and 192.168.10.1/255.255.255.255 specifies a host. There is no default.
  - Browse (...)—Browse for an IP address (instead or entering an IP address manually). Clicking Browse opens the Browse Source (or Destination) Address dialog box (Figure 2-13), on which you can select an already configured object or add, edit, or delete a selected object type. Selecting Add or Edit from the toolbar of the Browse Source Address dialog box opens the Add or Edit dialog box for the selected object type. Use this dialog box to enter or alter the Name, IP Address, and (optionally) the description for the entry.

Figure 2-13 Browse Source Address Dialog Box with Edit IP Name Dialog Box



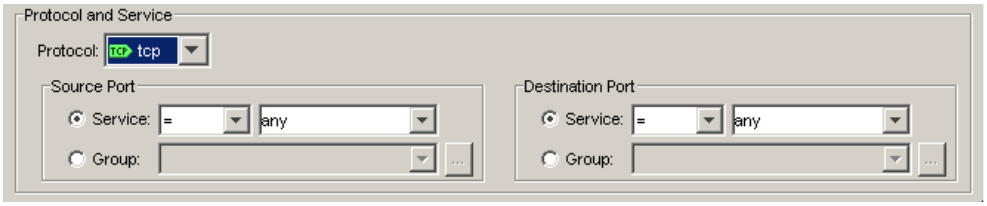
- Group Name—When you select Network Object Group in the Type field, you can select or browse (...) for a named group of networks and hosts (a network object group). There is no default.
- Interface—When you select Interface IP in the Type field, you can select an interface on which the host or network resides. The default is outside.

Managing Protocol and Service Groups

Service groups let you identify multiple non-contiguous port numbers that you want the ACL to match. For example, if you want to filter HTTP, FTP, and port numbers 5, 8, and 9, define a service group that includes all these ports. Without service groups, you would have to create a separate rule for each port. You can create service groups for TCP, UDP, IP, ICMP, and other IP protocols.

In the Protocol and Service area of the Add or Edit ACE dialog box, you configure the connection protocol and the type of service or the service group for the source and destination ports. If you do not want to make any changes, go on to the Description field. Figure 2-14 shows the Protocol and Service Area for the TCP protocol.

Figure 2-14 Protocol and Service Area, TCP protocol



You can associate multiple TCP or UDP services (ports) in a named group. You can then use the service group in an access or IPSec rule, a conduit, or other functions within ASDM and the CLI.

The term *service* refers to higher layer protocols associated with application level services having well known port numbers and “literal” names such as ftp, telnet, and smtp.

The security appliance permits the following TCP literal names: bgp, chargen, cmd, daytime, discard, domain, echo, exec, finger, ftp, ftp-data, gopher, h323, hostname, http, ident, irc, klogin, kshell, lpd, nntp, pop2, pop3, pptp, smtp, sqlnet, sunrpc, tacacs, talk, telnet, time, uucp, whois, www.

The **Name** of a service group must be unique across all types of object groups. For example, a **service** group and a **network** group may not share the same name.

Multiple service groups can be nested into a “group of groups” and used the same as a single group. When a service object group is deleted, it is removed from all service object groups where it is used.

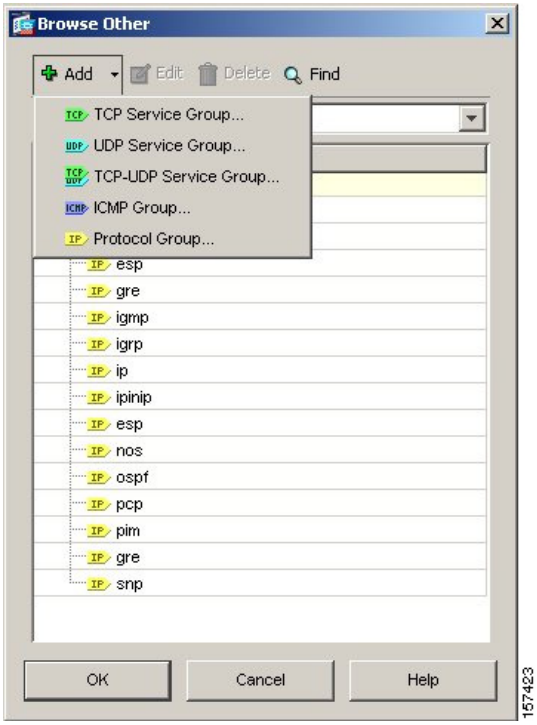
If a service group is used in an access rule, do not remove it. A service group used in an access rule cannot be made empty.

Use the Protocol and Service area to specify the protocol and type of service for this rule. The content of these areas depends on your protocol choice.

- Protocol—Select the protocol for the rule. Possible values are TCP, UDP, ICMP, IP, and IP Other. Depending on this choice, other fields might become available in this area.
  - If you select IP, no additional fields appear.
  - If you select IP Other, an Other area appears. In this area, you can select either Protocol or Protocol Group. Selecting Protocol enables a drop-down list, from which you can select a protocol. Selecting Protocol Group enables a drop-down list, from which you can select a

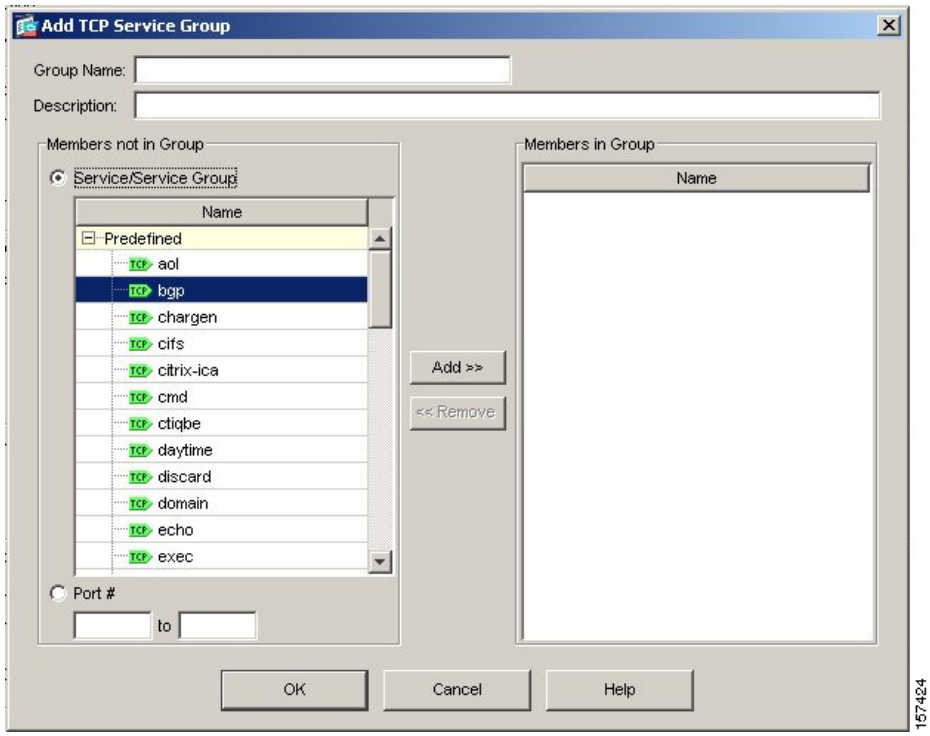
protocol group. Alternatively, you can click Browse (...), which opens the Browse Other dialog box (Figure 2-15), listing the names of the predefined IP protocols from which you can make a selection or create a new protocol service group.

Figure 2-15 Browse Other Dialog Box



Selecting one of the service groups in the Add menu opens the Add Service Group dialog box for the selected protocol. Figure 2-16 shows the Add TCP Service Group dialog box, which is representative of all the other such Add Service Group dialog boxes.

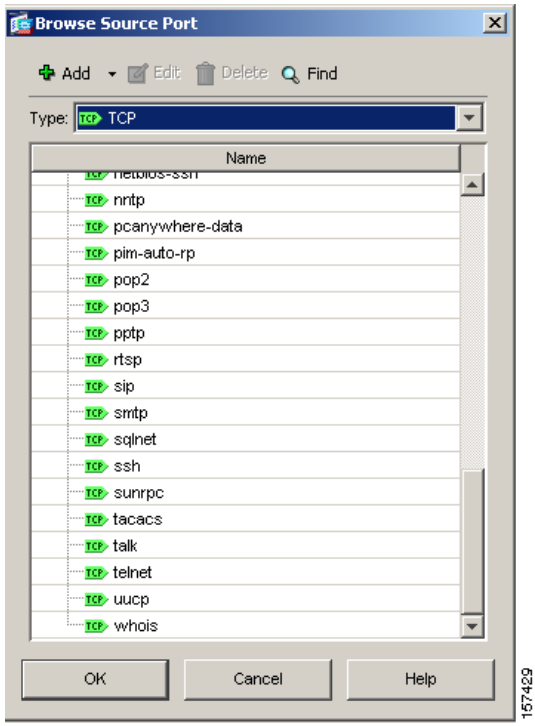
Figure 2-16 Add TCP Service Group Dialog Box



On this dialog box, you can specify a group name and description, then select a service/service group or a port/port range and add it to or remove it from the members in the group.

- Source/Destination Port—(TCP and UDP) If you select the Type as either TCP or UDP, the Source Port and Destination Port areas appear. Use the fields in these areas to specify a port number, a range of ports, or a well-known service name from a list of services, such as HTTP or FTP, that the ACL uses to match packets.
- Service—(TCP and UDP) The operator list specifies how the ACL matches the port. Choose one of the following operators: = (equals the port number), not = (does not equal the port number), > (greater than the port number), < (less than the port number), range (equal to one of the port numbers in the range).
- Group— (TCP and UDP) Select a service group from the drop-down list or click Browse (...), which opens the Browse Source (or Destination) Port dialog box (Figure 2-17), on which you can select, add, edit, or delete a source or destination port or create a source or destination port group.

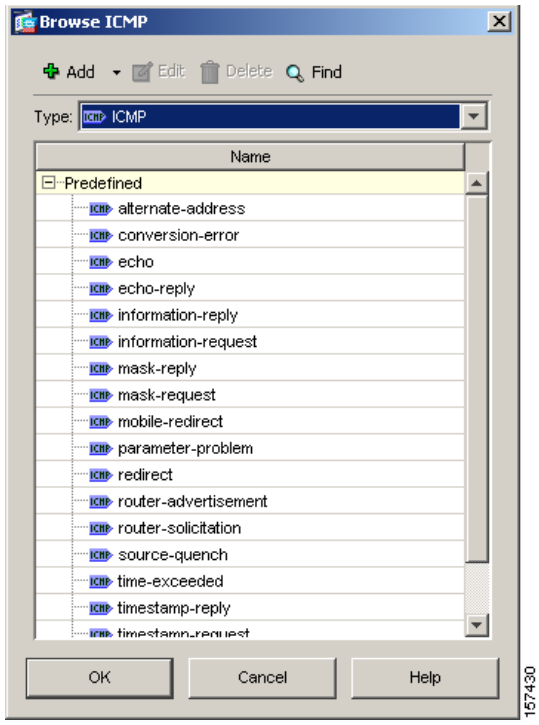
Figure 2-17 Browse Source Port



Selecting one of the service groups in the Add menu opens the Add Service Group dialog box for the selected protocol. Figure 2-16 shows the Add TCP Service Group dialog box, which is representative of all the other such dialog boxes.

– If you specify ICMP as the Type, the ICMP area appears. You can select ICMP Type and make a selection from the drop-down list or ICMP Group. If you select ICMP Group, you can either make a selection from the drop-down list or click Browse, which opens the Browse ICMP dialog box (Figure 2-18), on which you select an ICMP group from a preconfigured list.

Figure 2-18 Browse ICMP Dialog Box

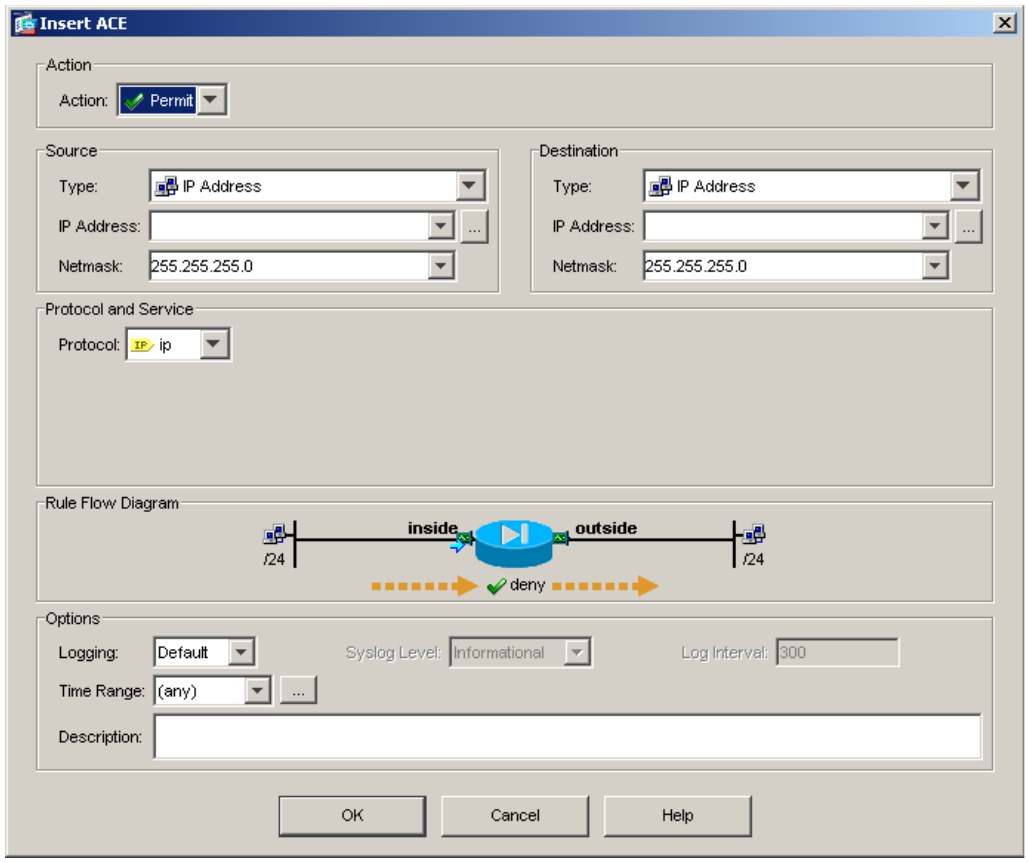


Selecting one of the service groups in the Add menu opens the Add Service Group dialog box for the selected protocol. Figure 2-16 shows the Add TCP Service Group dialog box, which is representative of all the other such dialog boxes.

Inserting ACL Rules

ACE rules are evaluated in the order in which they occur in the ACL Manager table. If you want to insert a rule into a particular place in the ACL Manager table, first select an existing ACE, then select Insert or Insert After from the Add menu.These selections respectively open the Insert ACE and Insert After ACE dialog boxes (Figure 2-19), on which you can specify the attributes of the ACE you want to create. These two dialog boxes are identical, except for the title. Insert places the new ACE above the selected ACE, and Insert After places the new ACE below the selected ACE.

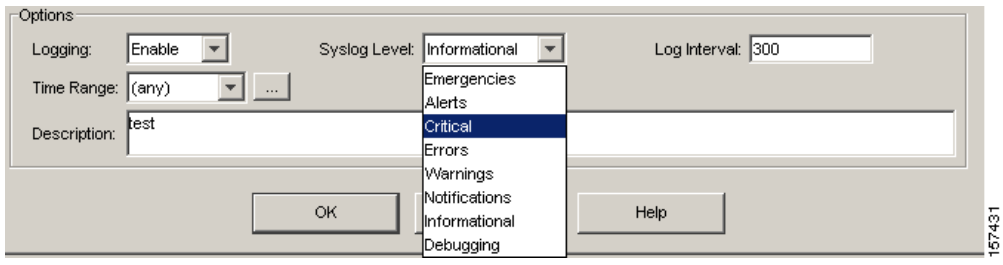
Figure 2-19 Insert ACE Dialog Box



Configuring Options

The Options dialog box lets you set options for each ACE rule. The fields in the Options area (Figure 2-20) set optional features for this rule, including logging parameters, time ranges, and description. Use the field descriptions below when setting these options.

Figure 2-20 Options Area, Add or Edit ACE Dialog Box



- Logging—Enables or disables logging or specifies the use of the default logging settings. If logging is enabled, the Syslog Level and Log Interval fields become available.

  When you enable logging, the security appliance generates a syslog message when a new flow is permitted or denied by the rule. Subsequent syslog messages are generated at the end of a log interval to summarize the hit count of the flow. The default interval is 300 seconds.

- Syslog Level—Selects the level of logging activity. The default is Informational.
- Log Interval—Specifies the interval for permit and deny logging. This is he amount of time the security appliance waits before sending the flow statistics to the syslog. This setting also serves as the timeout value for deleting a flow if no packets match the ACE. The default is 300 seconds. The range is 1 through 600 seconds.

Note Conduits and outbound lists do not support logging. See the online Help for Configuration > Properties > Logging > Logging Setup and subsequent windows for an explanation of how to set global logging options.

The default logging behavior is that if a packet is denied, then the security appliance generates log message 106023. If a packet is permitted, no syslog message appears. Select this option to return to the default logging behavior.

By default, syslog messages are generated at the informational level (level 6). You can select a different level of logging messages to be sent to the syslog server from the drop-down list in the Syslog Level field. Logging levels are as follows:

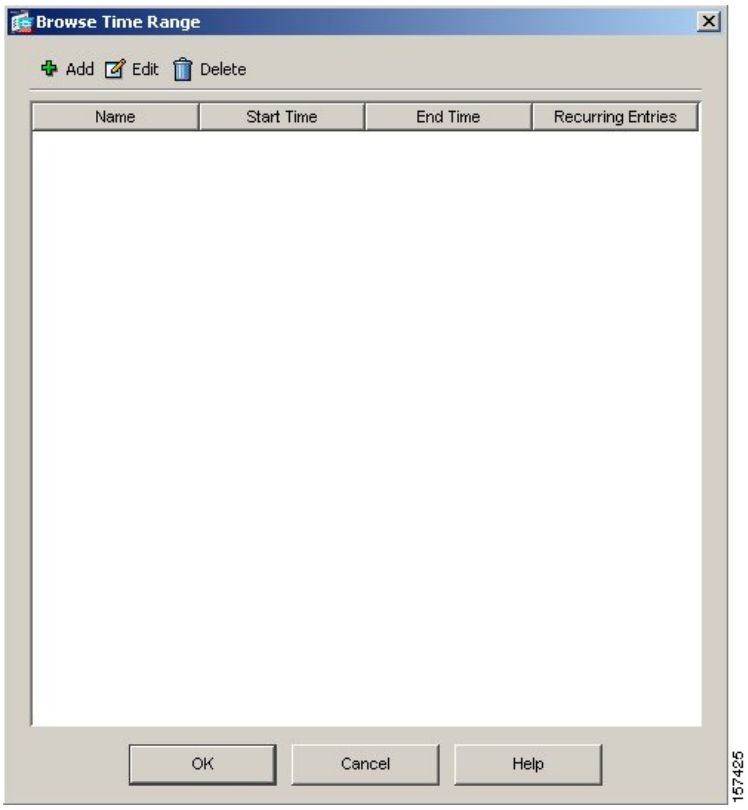
- Emergencies (level 0)—The security appliance does not use this level.
- Alert (level 1, immediate action needed)
- Critical (level 2, critical condition)
- Errors (level 3, error condition)
- Warnings (level 4, warning condition)
- Notifications (level 5, normal but significant condition)
- Informational (level 6, informational message only)
- Debugging (level 7, appears during debugging only)

If a packet matches the ACE, the security appliance creates a flow entry to track the number of packets received within a specific interval (see the description of the Logging Interval field). The security appliance generates a syslog message at the first hit and at the end of each interval, identifying the total number of hits during the interval. At the end of each interval, the security appliance resets the hit count to 0. If no packets match the ACE during an interval, the security appliance deletes the flow entry.

Note Logging consumes a certain amount of memory when enabled.

- Time Range—Selects the name of the time range to use with this rule. The default is (any). Click the Browse (...) button to open the Browse Time Range dialog box to select or add a time range (Figure 2-21).

Figure 2-21 Browse Time Range



A time range specifies the range of access hours during which a user can connect to the security appliance using this group policy.To add or edit a time range from the ACL configuration function, click Add or Edit on the Browse Time Range toolbar. The Add or Edit Time Range appears. Figure 2-22 shows the Add Time Range dialog box.

- Description—(Optional) Provides a brief description of this rule. A description line can be up to 100 characters long, but you can break a description into multiple lines.

Configuring General VPN Connection Settings Attributes

Follow the steps in this section to configure attributes that set the values of VPN connection attributes. These attributes control the number of simultaneous logins allowed, the timeouts, the name of the ACL to use for VPN connections, and the tunnel protocol. For all the attributes in this section, you can check the Inherit check box to allow the group policy to inherit a value from the default group policy.

Configuring Access Hours

The VPN access hours determine when users in this group can connect to the security appliance. To set the VPN access hours, you associate a group policy with a previously configured time-range policy, which determines the actual access hours.

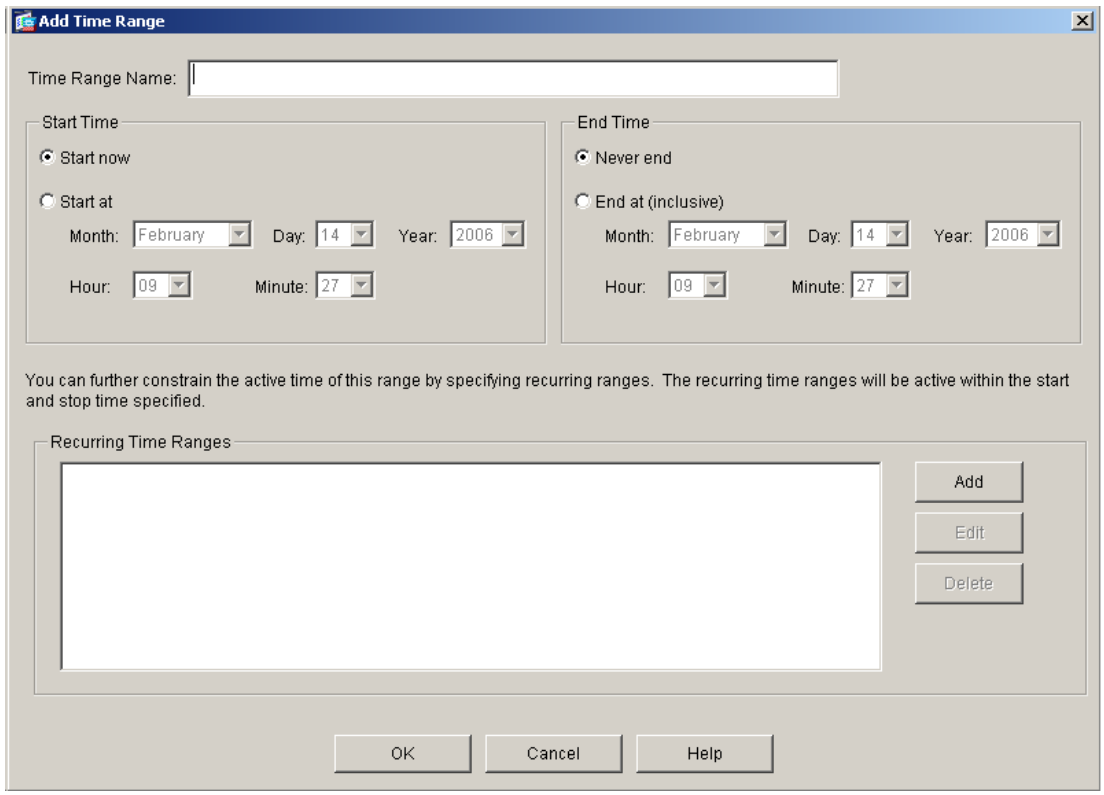
A time range is a variable specifying the range of access hours during which a user can connect to the security appliance using this group policy. You select the name of a time range from a menu when you want to restrict access hours.

To view the characteristics of the existing time ranges, select Configuration > Global Objects > Time Ranges. To select an existing time range to use with an ACL filter, choose a name from the drop-down Time Range menu in the Add/Edit ACE dialog box. To specify no time range restriction for this filter, choose **Unrestricted** from the menu. In either case, if you are not defining a new time range, skip to Configuring Simultaneous Logins, page 2-26.

You can check the Inherit check box to allow the group policy to inherit the access hours variable from the group policy. If you choose this option, skip to Configuring Simultaneous Logins, page 2-26.

To add or edit a time range from the General tab, clear the Inherit check box and click Manage. The Browse Time Range dialog box appears. Alternatively, you can get to the Browse Time Range dialog box by clicking Browse (...) in the Time Range area in the Add or Edit ACE dialog box. The Add or Edit Time Range dialog box appears (Figure 2-22). If you are editing an existing time range, the Time Range Name field is display-only.

Figure 2-22 Add Time Range Dialog Box

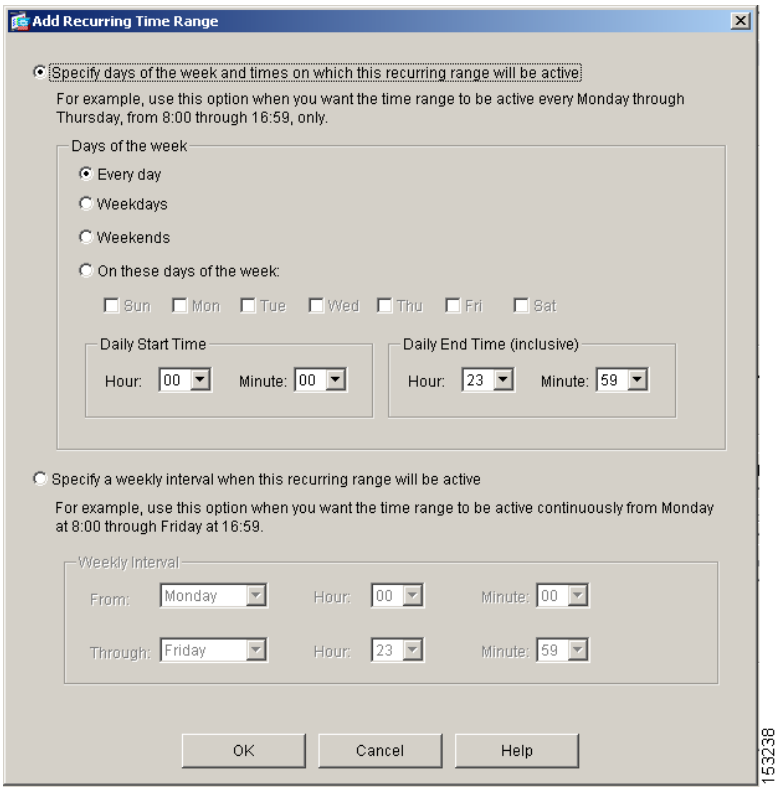


If you are adding a time range, specify a name for this time range. When needed, you select this time range by choosing this name from a drop-down list when you configure a group policy with a time range.

Specify the starting and ending times. If you configure specific starting and ending times, note that these times are inclusive.

You can further constrain the active time of this range by specifying recurring time ranges, which are active within the start and end times specified. To remove a recurring time range, select the range and click **Delete**. To add a recurring time range, click **Add** or select an existing time range and click **Edit**. The Add or Edit Recurring Time Ranges dialog box appears (Figure 2-23).

Figure 2-23 Add or Edit Recurring Time Ranges Dialog Box



Specify the recurring time ranges either as days of the week and times on which this recurring range is active or as a weekly interval when this recurring range is active, and click OK. Click OK to complete the configuration on the Add Time Range dialog box.

Configuring Simultaneous Logins

Specify the number of simultaneous logins allowed for any user. The default value is 3. The range is an integer in the range 0 through 2147483647. A group policy can inherit this value from another group policy. Enter 0 to disable login and prevent user access.

Caution While the maximum limit for the number of simultaneous logins is very large, allowing several could compromise security and affect performance.

Configuring Maximum Connect Time

Configure a maximum amount of time for VPN connections. At the end of this period of time, the security appliance terminates the connection. To allow unlimited connection time, check the Unlimited check box. To configure a specific time limit, clear the Unlimited check box. This makes the minutes field available. The minimum time is 1 minute, and the maximum time is 35791394 minutes. There is no default value.

Configuring User Idle Timeout

Configure the user idle timeout period by either checking the Unlimited check box or specifying a number of minutes that the system can remain idle. If there is no communication activity on the connection in this period, the security appliance terminates the connection. The minimum time is 1 minute, and the maximum time is 35791394 minutes. The default is 30 minutes.

Configuring WINS and DNS Servers and DHCP Scope

You can configure primary and secondary WINS servers and DNS servers and the DHCP scope. The default value in each case is none. To configure these attributes, do the following steps:

Step 1 Specify the primary and secondary DNS servers. The first IP address specified is that of the primary DNS server. The second (optional) IP address is that of the secondary DNS server. Leaving the first field blank instead of providing an IP address sets DNS servers to a null value, which allows no DNS servers and prevents inheriting a value from a default or specified group policy.

Every time that you enter a DNS Server value, you overwrite the existing setting. For example, if you configure the primary DNS server as 10.10.10.15 and later configure the primary DNS server to be 10.10.10.30, the later specification overwrites the first, and 10.10.10.30 becomes the primary DNS server.

Step 2 Specify the primary and secondary WINS servers. The first IP address specified is that of the primary WINS server. The second (optional) IP address is that of the secondary WINS server. Specifying the **none** keyword instead of an IP address sets WINS servers to a null value, which allows no WINS servers and prevents inheriting a value from a default or specified group policy.

Every time that you enter the **wins-server** command, you overwrite the existing setting. For example, if you configure WINS server x.x.x.x and then configure WINS server y.y.y.y, the second command overwrites the first, and y.y.y.y becomes the sole WINS server. The same is true for multiple servers. To add a WINS server rather than overwrite previously configured servers, include the IP addresses of all WINS servers when you enter this command.

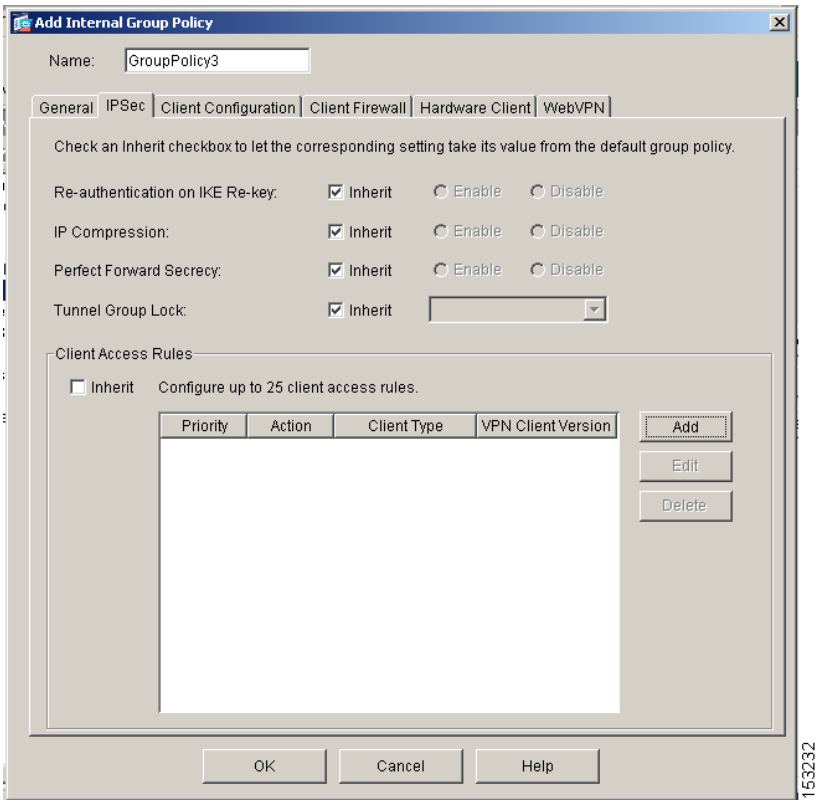
The following example shows how to configure WINS servers with the IP addresses 10.10.10.15 and 10.10.10.30 for the group policy named FirstGroup:

Step 3 Specify the DHCP scope; that is the range of servers IP addresses the security appliance DHCP server should use to assign addresses to users of this group policy. For example, to set an IP subnetwork of 10.10.85.0 (specifying the address range of 10.10.85.0 through 10.10.85.255) for the group policy, you would specify the DHCP scope as 10.10.85.0.

Configuring IPSec Attributes

The IPSec tab on the Add or Edit Internal Group Policy window lets you specify security attributes for this group policy. Figure 2-24 shows the IPSec tab.

Figure 2-24 Add Internal Group Policy Window, IPSec Tab



Check an Inherit check box to let the corresponding setting take its value from the default group policy. The following sections explain how to configure the attributes on this tab.

Configuring Reauthentication on IKE Rekey

Specify whether to require that users reauthenticate on IKE rekey by choosing Enable or Disable. If you enable reauthentication on IKE rekey, the security appliance prompts the user to enter a username and password during initial Phase 1 IKE negotiation and also prompts for user authentication whenever an IKE rekey occurs. Reauthentication provides additional security. Reauthentication on IKE rekey is disabled by default if you clear the Inherit check box.

If the configured rekey interval is very short, users might find the repeated authorization requests inconvenient. To avoid repeated authorization requests, disable reauthentication. To check the configured rekey statistics, select **Monitoring > VPN > VPN Statistics > Crypto Statistics** to view the security association statistics.

Note Reauthentication fails if there is no user at the other end of the connection.

Configuring IP Compression

Specify whether to enable IP compression, which is disabled by default. Enabling data compression might speed up data transmission rates for remote dial-in users connecting with modems. IP compression is disabled by default.

Caution Data compression increases the memory requirement and CPU usage for each user session and consequently decreases the overall throughput of the security appliance. For this reason, we recommend that you enable data compression only for remote users connecting with a modem. Design a group policy specific to modem users, and enable compression only for them.

To enable or disable LZS IP compression, select **Enable** or **Disable**.

Configuring Perfect Forward Secrecy

Specify whether to enable perfect forward secrecy. In IPSec negotiations, perfect forward secrecy ensures that each new cryptographic key is unrelated to any previous key. A group policy can inherit a value for perfect forward secrecy from the default group policy if you check the Inherit check box. Otherwise, perfect forward secrecy is disabled by default. To enable or disable perfect forward secrecy, select **Enable** or **Disable**.

Configuring Tunnel Group Locking

Specify whether to restrict remote users to access only through the tunnel group, by enabling or disabling the Tunnel Group Lock attribute.

On the Add or Edit Internal Group Policy, IPSec tab, uncheck the Inherit check box and select a tunnel-group name from the drop-down list. Users associated with this group policy are then allowed access only through the specified tunnel group.

The tunnel-group name specifies the name of an existing tunnel group that the security appliance requires for the user to connect. Tunnel group lock restricts users by checking whether the group configured in the VPN client is the same as the tunnel group to which the user is assigned. If it is not, the security appliance prevents the user from connecting. If you do not configure tunnel group lock, the security appliance authenticates users without regard to the assigned group. Group locking is disabled by default.

To remove group locking from the group-policy configuration, select None from the list. This option sets the group lock to a null value, thereby allowing no group-lock restriction. It also prevents inheriting a group-lock value from a default or specified group policy.

Configuring Client Access Rules

The Client Access Rules area lets you specify up to 25 rules that determine whether to permit or deny access by certain types and versions of VPN clients. Either the group policy can inherit these rules from the default group policy, or you can specify particular rules for this group policy.

The table in this area shows the priority, action, client type and VPN client version that each rule specifies.

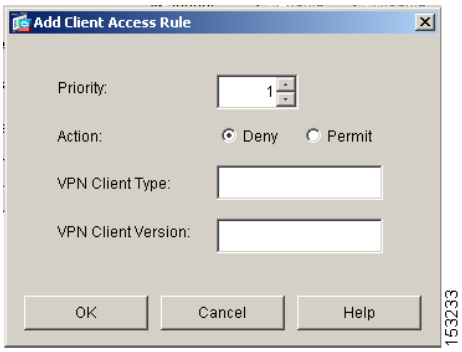
To configure rules that limit the remote access client types and versions that can connect via IPSec through the security appliance, clear the **Inherit** check box. This makes the buttons associated with the table active. By default, there are no access rules. When there are no client access rules, all client types and versions can connect. To delete individual rules, click **Delete**.

The columns in the Client Access Rules table are as follows:

- Priority—Shows the priority for this rule. Determines the priority of the rule. The rule with the lowest integer has the highest priority. Therefore, the rule with the lowest integer that matches a client type and/or version is the rule that applies. If a lower priority rule contradicts, the security appliance ignores it.
- Action—Specifies whether this rule permits or denies access for clients of a particular type and version.
- Client Type—Specifies the type of VPN client to which this rule applies, software or hardware, and for software clients, all Windows clients or a subset. Identifies device types via free-form strings, for example VPN 3002. A string must match exactly its appearance in the show vpn-sessiondb remote display, except that you can use the * character as a wildcard.
- VPN Client Version —Specifies the version or versions of the VPN client to which this rule applies. This box contains a comma-separated list of software or firmware images appropriate for this client. Identifies the device version via free-form strings, for example 7.0. A string must match exactly its appearance in the show vpn-sessiondb remote display, except that you can use the * character as a wildcard.

To add a new rule for an IPSec group policy, click **Add**. To modify an existing rule for an IPSec group policy, click **Edit**. The Add or Edit Client Access Rule dialog box appears (Figure 2-25).

Figure 2-25 Add Client Access Rule Dialog Box



Construct rules according to these caveats:

- If you do not define any rules, the security appliance permits all connection types.
- When a client matches none of the rules, the security appliance denies the connection. This means that if you define a deny rule, you must also define at least one permit rule, or the security appliance denies all connections.
- For both software and hardware clients, type and version must match exactly their appearance in the **Monitoring > VPN > VPN Statistics > Sessions** window.
- The * character is a wildcard, which you can use multiple times in each rule. For example, specifying the VPN client version as **version 3.*** in a client access rule applies that rule to the specified client type running release versions 3.x software.
- You can construct a maximum of 25 rules per group policy.

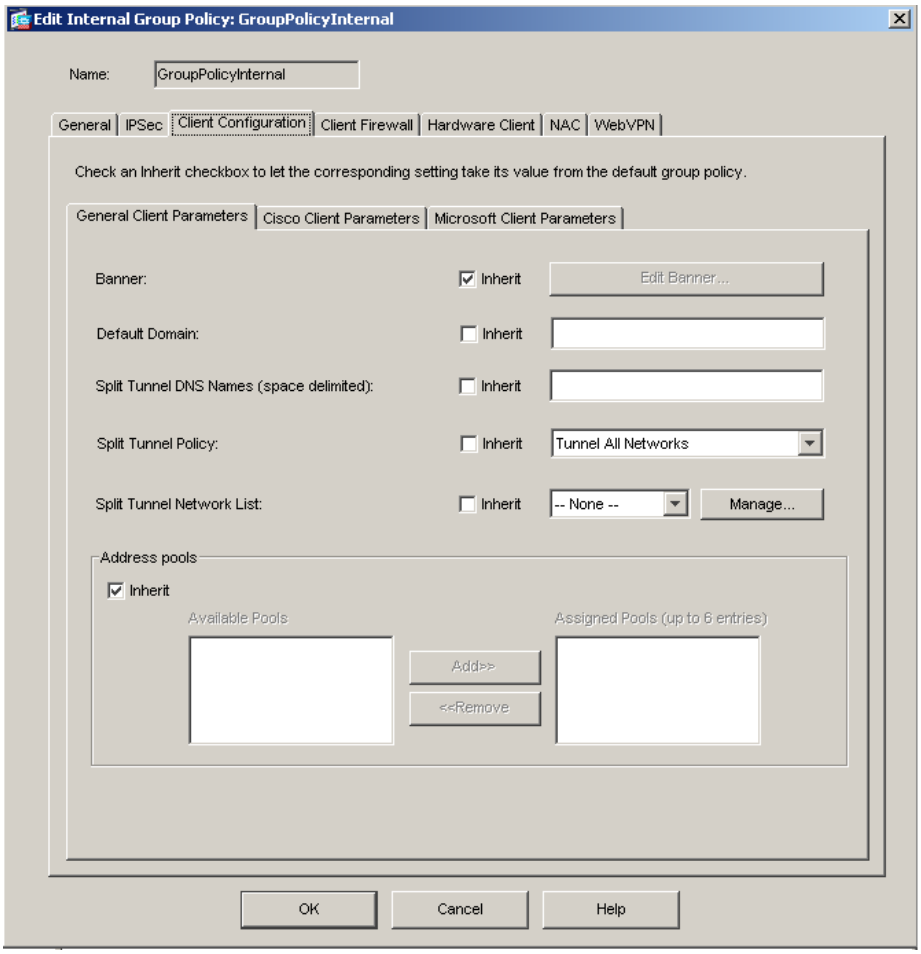
- There is a limit of 255 characters for an entire set of rules.
- You can use n/a for clients that do not send client type and/or version.

Configuring Client Configuration Parameters

The Client Configuration tab of the Add/Edit Internal Group Policy Window (Figure 2-26) consists of the following tabs:

- General Client parameters
- Cisco Client parameters
- Microsoft Client parameters

Figure 2-26 General Client Parameters Tab

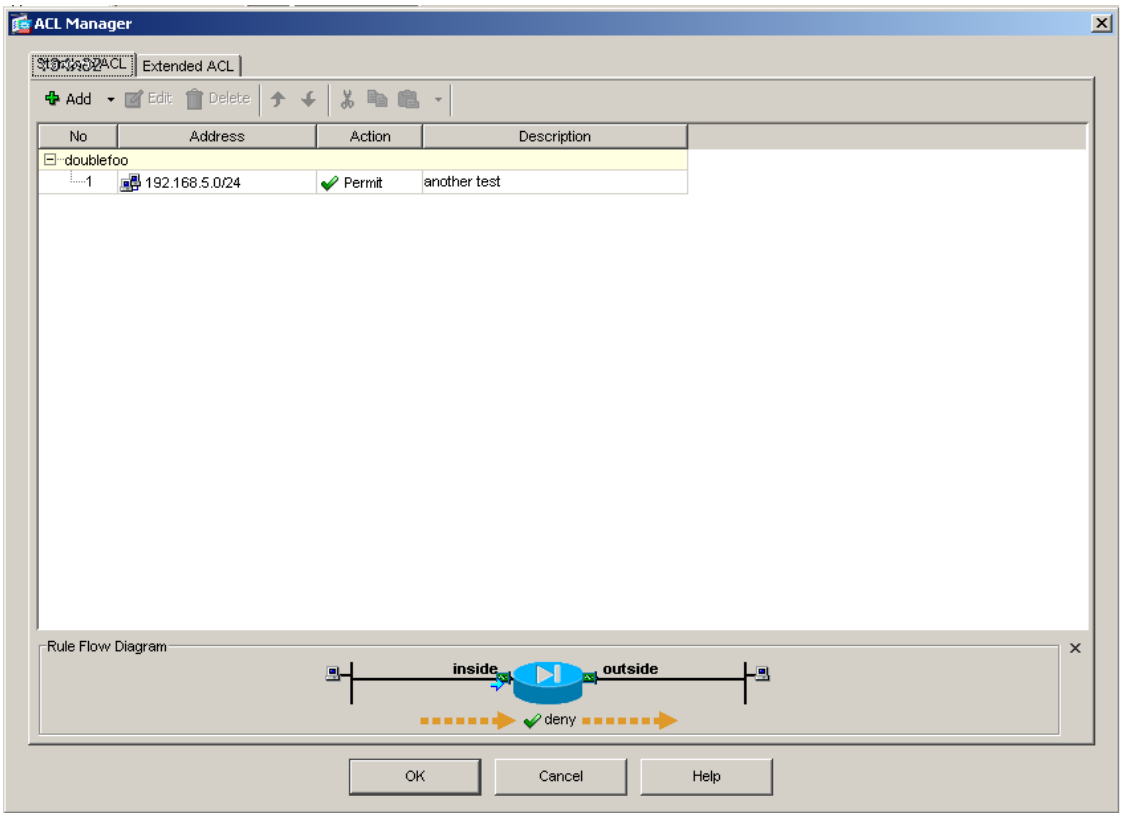


Configuring General Client Parameters

The General Client Parameters tab configures client attributes that are common across both Cisco and Microsoft clients, including the banner text, default domain, split tunnel parameters, and address pools. In most cases, you can use the Inherit check box (checked by default) to indicate that the corresponding setting takes its value from the default group policy. Clearing the Inherit check box makes other options available for the parameter. Use the following field descriptions when configuring the general client parameters:

- Banner—Specifies whether to inherit the banner from the default group policy or enter new banner text.
- Edit Banner—Displays the View/Config Banner dialog box, in which you can enter banner text, up to 500 characters. See Configuring the Banner Message, page 2-33 for more information.
- Default Domain—Specifies whether to inherit the default domain from the default group policy or use a new default domain specified in the field. See Configuring Domain Attributes for Tunneling for more information about this and the following tunneling-related fields.
- Split Tunnel DNS Names (space delimited)—Specifies whether to inherit the split-tunnel DNS names or from the default group policy or specify a new name or list of names in the field.
- Split Tunnel Policy—Specifies whether to inherit the split-tunnel policy from the default group policy or select a policy from the menu. The menu options are to tunnel all networks, tunnel those in the network list below, or exclude those in the network list below.
- Split Tunnel Network List—Specifies whether to inherit the split-tunnel network list from the default group policy or select from the drop-down list.
- Manage—Opens the ACL Manager dialog box (Figure 2-27), on which you can manage standard and extended access control lists.

Figure 2-27 ACL Manager Dialog Box, with Standard and Extended ACLs



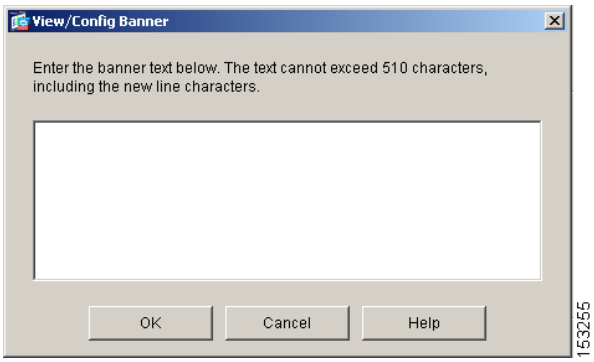
This ACL Manager dialog box is functionally identical to the one described in Managing ACLs and ACEs, although the standard and extended ACLs are on two different tabs in this case.

- Address Pools—Configures the address pools available through this group policy.
  - Available Pools—Specifies a list of address pools for allocating addresses to remote clients. Deselecting the Inherit check box with no address pools in the Assigned Pools list indicates that no address pools are configured and disables inheritance from other sources of group policy.
  - Add—Moves the name of an address pool from the Available Pools list to the Assigned Pools list.
  - Remove—Moves the name of an address pool from the Assigned Pools list to the Available Pools list.
  - Assigned Pools (up to 6 entries)—Lists the address pools you have added to the assigned pools list. The address-pools settings in this table override the local pool settings in the group. You can specify a list of up to six local address pools to use for local address allocation. The order in which you specify the pools is significant. The security appliance allocates addresses from these pools in the order in which the pools appear in this command.

Configuring the Banner Message

The banner is a message that is displayed to remote clients when they connect. The default is no banner. If you choose not to inherit the banner from the default group policy, clear the Inherit check box and click Edit Banner. The View/Config Banner dialog box appears (Figure 2-28).

Figure 2-28 View/Config Banner Dialog Box



To specify the banner, or welcome message, if any, that you want to display, enter the banner text, up to 510 characters in length. Enter the "\n" sequence to insert a carriage return.

Note A carriage-return/line-feed included in the banner counts as two characters.

To delete a banner, remove the text.

Configuring Domain Attributes for Tunneling

You can specify a default domain name for tunneled packets or a list of domains to be resolved through the split tunnel. The following sections describe how to set these domains.

Defining a Default Domain Name for Tunneled Packets

The security appliance passes the default domain name to the IPSec client to append to DNS queries that omit the domain field. When there are no default domain names, users inherit the default domain name in the default group policy. To specify the default domain name for users of the group policy, clear the Inherit check box and enter the default domain name in the field.

The domain name that you enter identifies the default domain name for the group. To specify that there is no default domain name, leave this field blank. This command sets a default domain name with a null value, which disallows a default domain name and prevents inheriting a default domain name from a default or specified group policy.

Defining a List of Domains for Split Tunneling

To provide a list of domains for split-tunneling, clear the Inherit check box and enter a space-delimited list of domains to be resolved through the split tunnel. When there are no split tunneling domain lists, users inherit any that exist in the default group policy. To prevent users from inheriting such split tunneling domain lists, leave this list blank.

The domain name attribute provides a domain name that the security appliance resolves through the split tunnel. Leaving this list blank indicates that there is no split DNS list. It also sets a split DNS list with a null value, thereby disallowing a split DNS list, and prevents inheriting a split DNS list from a default or specified group policy.

Enter a single space to separate each entry in the list of domains. There is no limit on the number of entries, but the entire string can be no longer than 255 characters. You can use only alphanumeric characters, hyphens (-), and periods (.). If the default domain name is to be resolved through the tunnel, you must explicitly include that name in this list.

Configuring Split-Tunneling Attributes

Split tunneling lets a remote-access IPSec client conditionally direct packets over an IPSec tunnel in encrypted form or to a network interface in clear text form. With split tunneling enabled, 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. This command applies this split tunneling policy to a specific network.

Setting the Split-Tunneling Policy

Set the rules for tunneling traffic by specifying the split-tunneling policy. The default is to tunnel all traffic. To set a split tunneling policy, clear the Inherit check box and select the split-tunnel policy from the drop-down menu. To remove the split-tunnel policy attribute from the running configuration, leave this field blank. This enables inheritance of a value for split tunneling from another group policy.

- Select Tunnel All Networks to specify that no traffic goes in the clear or to any other destination than the security appliance. This, in effect, disables split tunneling. Remote users reach Internet networks through the corporate network and do not have access to local networks. This is the default option.
- Select Tunnel Network List Below to tunnel all traffic from or to the specified networks. This option enables split tunneling. It lets you create a network list of addresses to tunnel. Data to all other addresses travels in the clear and is routed by the remote user's Internet service provider.
- Select Exclude Network List Below to define a list of networks to which traffic goes in the clear. This feature is useful for remote users who want to access devices on their local network, such as printers, while they are connected to the corporate network through a tunnel. This option applies only to the Cisco VPN client.

Note Split tunneling is primarily a traffic management feature, not a security feature. For optimum security, we recommend that you do not enable split tunneling.

Creating a Network List for Split-Tunneling

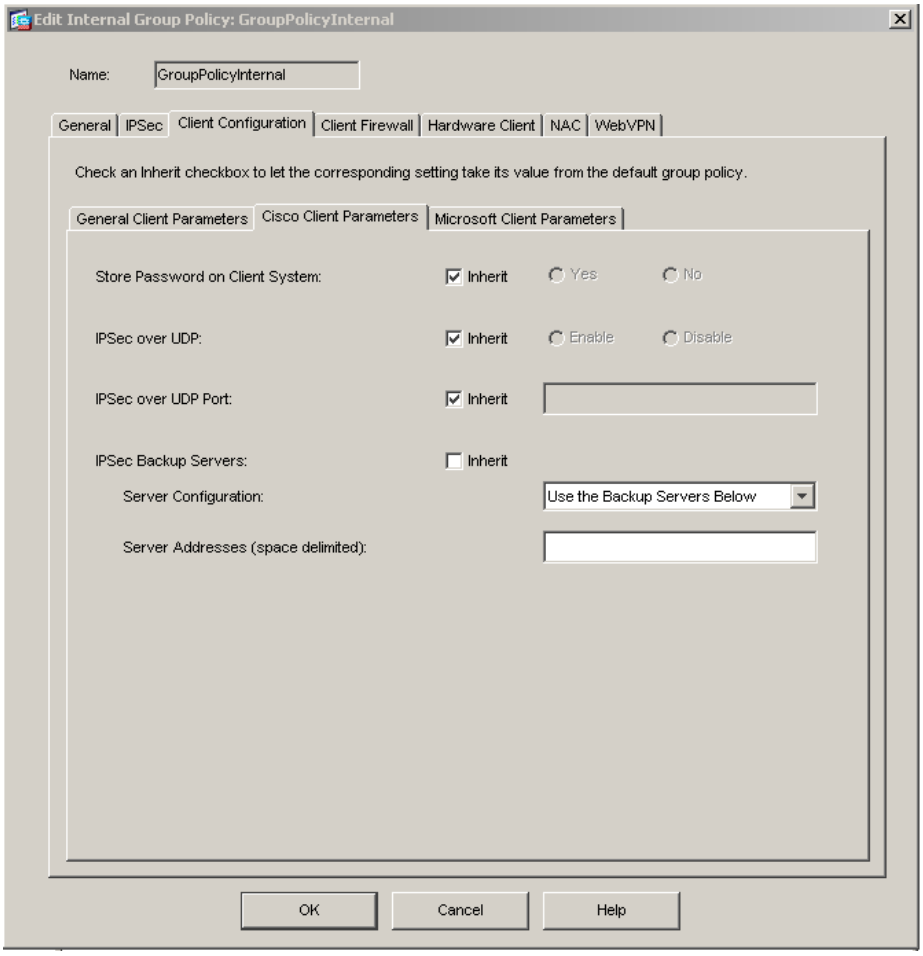
Select a network list name for split tunneling from the Split Tunnel Network List drop-down menu. Split tunneling network lists distinguish networks that require traffic to travel across the tunnel from those that do not require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, which is an ACL that consists of a list of addresses on the private network. Only standard-type ACLs are allowed. Clicking **Manage** opens the ACL Manager dialog box, where you can configure the ACLs. For information on using ACL Manager dialog box, see Configuring the ACL Filter, page 2-12.

The access-list name that you select identifies an access list that enumerates the networks to tunnel or not tunnel. Selecting **None** indicates that there is no network list for split tunneling; the security appliance tunnels all traffic. Selecting **None** sets a split tunneling network list with a null value, thereby disallowing split tunneling. It also prevents inheriting a default split tunneling network list from a default or specified group policy.

Configuring Cisco Client Parameters

The attributes on the Cisco Client Parameters tab (Figure 2-29) specify certain security settings for the group, including password storage, IPSec over UPD settings, and IPSec backup servers.

Figure 2-29 Cisco Client Parameters Tab



Configuring Password Storage

You can specify whether to let users store their login passwords on the client system. For security reasons, password storage is disabled by default. Enable password storage only on systems that you know to be in secure sites.

To enable or disable password storage, clear the Inherit check box for the Store Password on Client System attribute and select either **Yes** (enable) or **No** (disable).

This action does not apply to interactive hardware client authentication or individual user authentication for hardware clients.

Configuring IPSec-UDP Attributes

IPSec over UDP, sometimes called IPSec through NAT, lets a Cisco VPN client or hardware client connect via UDP to a security appliance that is running NAT. It is disabled by default. IPSec over UDP is proprietary; it applies only to remote-access connections, and it requires mode configuration. The security appliance exchanges configuration parameters with the client while negotiating SAs. Using IPSec over UDP may slightly degrade system performance.

To enable or disable **IPSec over UDP**, clear the Inherit check box and choose either **Enable** or **Disable**.

The Cisco VPN client must also be configured to use IPSec over UDP (it is configured to use it by default). The VPN 3002 requires no configuration to use IPSec over UDP.

To use IPSec over UDP, you must also configure the **IPSec over UDP Port** attribute, which sets a UDP port number for IPSec over UDP. In IPSec negotiations, the security appliance listens on the configured port and forwards UDP traffic for that port even if other filter rules drop UDP traffic. To configure the IPSec over UDP Port attribute, clear the Inherit check box and enter a port number into the field. The port numbers can range from 4001 through 49151. The default port value is 10000.

Configuring IPSec Backup Servers

Configure backup servers if you plan on using them. IPSec backup servers let a VPN client connect to the central site when the primary security appliance is unavailable.When you configure backup servers, the security appliance pushes the server list to the client as the IPSec tunnel is established. Backup servers do not exist until you configure them, either on the client or on the primary security appliance.

Configure backup servers either on the client or on the primary security appliance. If you configure backup servers on the security appliance, it pushes the backup server policy to the clients in the group, replacing the backup server list on the client if one is configured.

Note If you are using hostnames, it is wise to have backup DNS and WINS servers on a separate network from that of the primary DNS and WINS servers. Otherwise, if clients behind a hardware client obtain DNS and WINS information from the hardware client via DHCP, and the connection to the primary server is lost, and the backup servers have different DNS and WINS information, clients cannot be updated until the DHCP lease expires. In addition, if you use hostnames and the DNS server is unavailable, significant delays can occur.

To specify one or more backup servers or to remove the configured backup server or servers from the client configuration, do the following:

Step 1 Clear the Inherit check box.

Step 2 Select one of the following options from the drop-down menu:

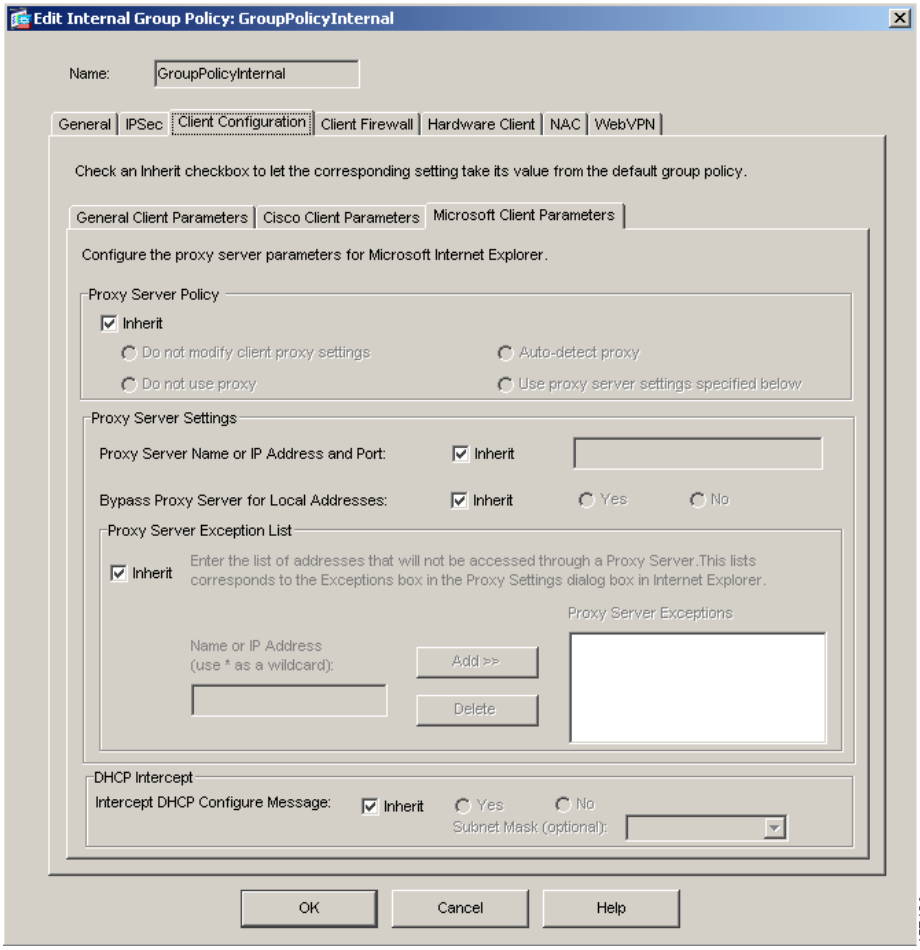
- Keep Client Configuration— Specifies that the security appliance sends no backup server information to the client. The client uses its own backup server list, if configured. This is the default.
- Clear Client Configuration—Specifies that the client uses no backup servers. The security appliance pushes a null server list.
- Use the Backup Servers Below—Specifies that you want to configure a list of servers to use if the primary security appliance is unavailable.

Step 3 If you select Use the Backup Servers Below, you must fill in one or more server addresses in the Server Addresses field. This list is a space-delimited, priority-ordered list of servers for the VPN client to use when the primary security appliance is unavailable. This list identifies servers by IP address or hostname. The list can be 500 characters long, and it can contain up to10 entries.

Configuring Microsoft Client Parameters

The Microsoft Client Parameters tab (Figure 2-30) configures client attributes that are specific to Microsoft clients, specifically, proxy server parameters for Microsoft Internet Explorer.

Figure 2-30 Microsoft Client Parameters Tab



Use the fields on this tab to configure parameters specific to Microsoft clients:

- Proxy Server Policy—Configures the Microsoft Internet Explorer browser proxy actions (“methods”) for a client PC.
  - Do not modify client proxy settings—Leaves the HTTP browser proxy server setting in Internet Explorer unchanged for this client PC.
  - Do not use proxy—Disables the HTTP proxy setting in Internet Explorer for the client PC.

  - Auto-detect proxy—Enables the use of automatic proxy server detection in Internet Explorer for the client PC.
  - Use proxy server settings specified below—Sets the HTTP proxy server setting in Internet Explorer to use the value configured in the Proxy Server Name or IP Address field.

- Proxy Server Settings—Configures the proxy server parameters for Microsoft clients using Microsoft Internet Explorer.
  - Proxy Server Name or IP Address—Specifies the IP address or name of an Microsoft Internet Explorer server that is applied for this client PC.

Note ASDM lets you configure the proxy server name or IP address. To configure the optional port to use, as well as the server, you must use the **msie-proxy server** command in group-policy configuration mode.

  - Bypass Proxy Server for Local Addresses— Configures Microsoft Internet Explorer browser proxy local-bypass settings for a client PC. Select Yes to enable local bypass or No to disable local bypass.
  - Proxy Server Exception List—Configures Microsoft Internet Explorer browser proxy exception list settings for a local bypass on the client PC. Enter the list of addresses that you do not want to have accessed through a proxy server. This list corresponds to the Exceptions box in the Proxy Settings dialog box in Internet Explorer.
  - Name or IP Address (use * as a wildcard)—Specifies the IP address or name of an MSIE server that is applied for this client PC.
  - Add—Add the specified name or IP address to the Proxy Server Exceptions list.
  - Delete—Remove the specified name or IP address from the Proxy server Exceptions list.
  - Proxy Server Exceptions—Lists the server names and IP addresses that you want to exclude from proxy server access. This list corresponds to the Exceptions box in the Proxy Settings dialog box in Internet Explorer.

- DHCP Intercept—Enables or disables DHCP Intercept. DHCP Intercept lets Microsoft XP clients use split-tunneling with the security appliance. The security appliance replies directly to the Microsoft Windows XP client DHCP Inform message, providing that client with the subnet mask, domain name, and classless static routes for the tunnel IP address. For Windows clients prior to XP, DHCP Intercept provides the domain name and subnet mask. This is useful in environments in which using a DHCP server is not advantageous.

Note A Microsoft XP anomaly results in the corruption of domain names if split tunnel options exceed 255 bytes. To avoid this problem, the security appliance limits the number of routes it sends to 27 to 40 routes, with the number of routes dependent on the classes of the routes.

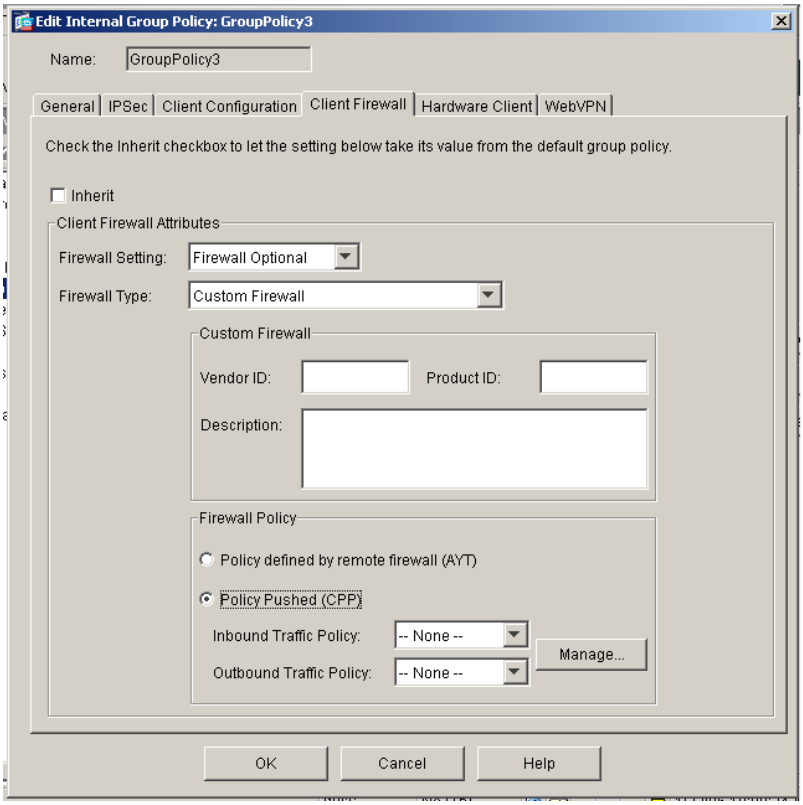
  - Intercept DHCP Configure Message—Specifies whether to inherit the DHCP intercept policy from the group policy or to enable (Yes) or disable (No) DHCP policy.
  - Subnet Mask (optional)—Selects the subnet mask from the drop-down list.

Configuring Firewall Attributes

A *firewall* isolates and protects a computer from the Internet by inspecting each inbound and outbound individual packet of data to determine whether to allow or drop it. Firewalls provide extra security if remote users in a 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 to the security appliance with the VPN client can choose the appropriate firewall option. When there are no firewall policies, users inherit any that exist in the default or other group policy.

Set personal firewall policies that the security appliance pushes to the VPN client during IKE tunnel negotiation on the Client Firewall tab (Figure 2-31).

Figure 2-31 Edit Internal Group Policy Client Firewall Tab



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

The following examples illustrate the use of the client firewall.

In the first scenario, 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 security appliance. (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, each user can customize his or her own configuration.

In the second scenario, 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 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 security appliance, you create a set of traffic management rules to enforce on the VPN client, associate those rules with a filter, and designate that filter as the firewall policy. The security appliance pushes this policy down to the VPN client. The VPN client then in turn passes the policy to the local firewall, which enforces it.

The Add or Edit Internal Group Policy window, Client Firewall tab, lets you configure firewall settings for VPN clients for the group policy being added or modified. To specify the client firewall settings, clear the Inherit check box and configure the following attributes in the Client Firewall Attributes area

Configuring Firewall Setting

Specify whether there is no firewall, or whether the firewall is optional or required by selecting the appropriate setting from the drop-down menu.

Note If you have remote users in this group who do not yet have firewall capacity, choose **Firewall Optional**. The **Firewall Optional** setting allows all the users in the group to connect. Those who have a firewall can use it; users that connect without a firewall receive a warning message. This setting is useful if you are creating a group in which some users have firewall support and others do not—for example, you may have a group that is in gradual transition, in which some members have set up firewall capacity and others have not yet done so.

Configuring Firewall Type

Select the type of firewall (or no firewall) from the drop-down menu. The options are:

- No Firewall—Indicates that there is no client firewall policy and prevents inheriting a firewall policy from a default or specified group policy.
- Cisco Integrated Firewall—Selects the Cisco Integrated Firewall type.
- Cisco Security Agent—Selects the Cisco Intrusion Prevention Security Agent firewall type.
- Zone Labs Firewalls—Selects either the Zone Labs Zone Alarm or the Zone Alarm Pro firewall type or both.
- Sygate Personal Firewalls—Selects either the Sygate Personal firewall type, the Sygate Personal Pro firewall type, or the Sygate Security Agent firewall type.
- Network ICE, Black ICE Firewall—Selects the Network ICE Black ICE firewall type.
- Custom Firewall—Indicates that this policy uses a custom firewall. With this selection, the Custom Firewall and Firewall Policy areas become active.

Configuring a Custom Firewall

If you selected Custom Firewall as the firewall type, you must also configure the custom firewall attributes, as follows:

- Vendor ID—Identifies the firewall vendor.

- Product ID—Identifies the model or product name of the firewall product.
- Description—Optionally provides additional information about the custom firewall.

Configure the Firewall Policy attributes to specify the source and characteristics of the firewall policy, as follows:

- Policy defined by remote firewall (AYT)—Specifies that the policy is to use the firewall installed on the remote user PC and, after the connection is established, polls that firewall every 30 seconds to ensure that it is running. This is the "Are You There" or AYT mechanism. The local firewall enforces the firewall policy on the VPN client. The security appliance allows VPN clients in this group to connect only if they have the designated firewall installed and running. If the designated firewall is not running, the connection fails.
- Policy Pushed (CPP)—Enforces a centralized firewall policy for personal firewalls on VPN client PCs. This firewall policy is called "push policy" or Central Protection Policy, because the policy is pushed from the peer. If you select this option, the Inbound Traffic Policy and Outbound Traffic Policy lists and the Manage button become active.The security appliance enforces on the VPN clients in this group the traffic management rules defined by the filter you choose from the Policy Pushed (CPP) drop-down menu. The choices available on the menu are filters defined on this security appliance, including the default filters. Keep in mind that the security appliance pushes these rules down to the VPN client, so you should create and define these rules relative to the VPN client, not the security appliance. For example, "in" and "out" refer to traffic coming into the VPN client or going outbound from the VPN client. If the VPN client also has a local firewall, the policy pushed from the security appliance works with the policy of the local firewall. Any packet that is blocked by the rules of either firewall is dropped.

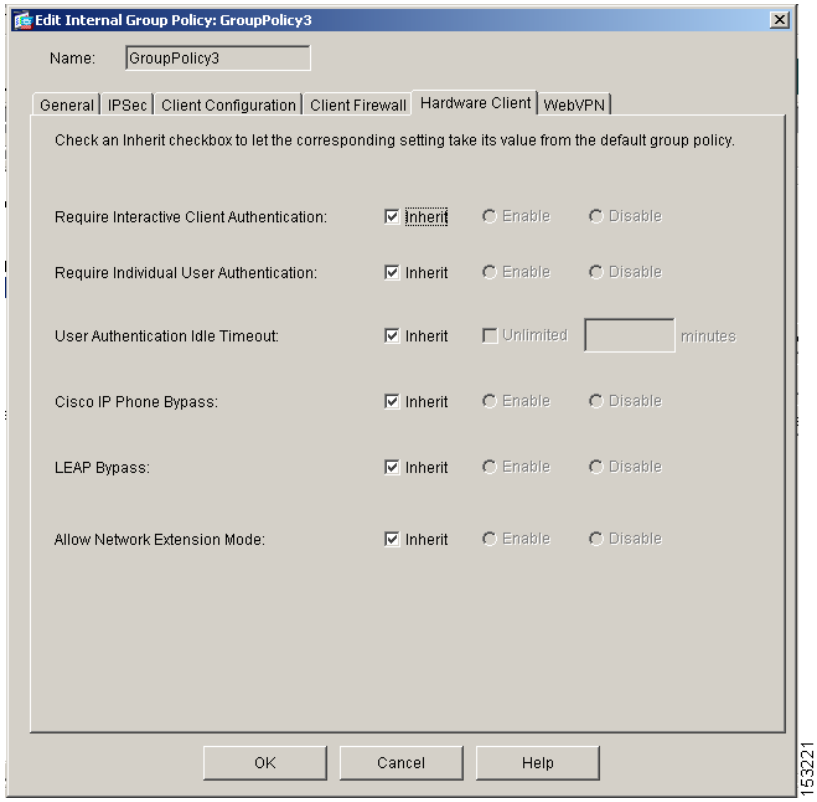
If you select Policy Pushed (CPP), you must also select the policies that the client uses for inbound and outbound traffic.

Clicking **Manage** opens the ACL Manager dialog box (Figure 2-9), i n which you can create a set of traffic management rules to enforce on the VPN client, associate those rules with a filter, and designate that filter as the firewall policy. The security appliance pushes this policy down to the VPN client, which, in turn, passes the policy to the local firewall, which enforces it.

Configuring Attributes for VPN Hardware Clients

The Add or Edit Internal Group Policy Hardware Client tab (Figure 2-32) lets you configure attributes specific to VPN hardware clients. On this tab you can enable or disable secure unit authentication and user authentication and set a user authentication timeout value for VPN hardware clients. You can also allow Cisco IP phones and LEAP packets to bypass individual user authentication and allow hardware clients using Network Extension Mode to connect.

Figure 2-32 Edit Internal Group Policy Hardware Client Tab



Requiring Interactive Client Authentication (Secure Unit Authentication)

Secure unit authentication provides additional security by requiring VPN hardware clients to authenticate with a username and password each time that the client initiates a tunnel. With this feature enabled, the hardware client does not have a saved username and password. Secure unit authentication is disabled by default.

Note With this feature enabled, to bring up a VPN tunnel, a user must be present to enter the username and password.

Secure unit authentication requires that you have an authentication server group configured for the tunnel group the hardware client(s) use. If you require secure unit authentication on the primary security appliance, be sure to configure it on any backup servers as well.

Interactive hardware client authentication provides additional security by requiring the VPN 3002 Hardware Client to authenticate with a username and password that you enter manually each time the VPN 3002 initiates a tunnel. With this feature enabled, the VPN 3002 does not have a saved username and password. When you enter the username and password, the VPN 3002 sends these credentials to the security appliance to which it connects. The security appliance facilitates authentication, on either the internal or an external authentication server. If the username and password are valid, the tunnel is established.

When you enable interactive hardware client authentication for a group, the security appliance pushes that policy to the VPN 3002s in the group. If you have previously set a username and password on the VPN 3002, the software deletes them from the configuration file. When you try to connect, the software prompts you for a username and password.

If, on the security appliance, you subsequently disable interactive hardware authentication for the group, it is enabled locally on the VPN 3002s, and the software continues to prompt for a username and password. This lets the VPN 3002 connect, even though it lacks a saved username and password, and the security appliance has disabled interactive hardware client authentication. If you subsequently configure a username and password, the feature is disabled, and the prompt no longer displays. The VPN 3002 connects to the security appliance using the saved username and password.

Specify whether to enable or disable the requirement for interactive client authentication by clearing the Inherit check box and selecting either **Enable** or **Disable**. This parameter is disabled by default.

Requiring Individual User Authentication

When enabled, user authentication requires that individual users behind a hardware client authenticate to gain access to the network across the tunnel. Individual users authenticate according to the order of authentication servers that you configure. Individual user authentication for these users is disabled by default. To display a banner to VPN 3002 devices in a group, individual user authentication must be enabled.

If you require user authentication on the primary security appliance, be sure to configure it on any backup servers as well.

Individual user authentication protects the central site from access by unauthorized persons on the private network of the VPN 3002. When you enable individual user authentication, each user that connects through a VPN 3002 must open a web browser and manually enter a valid username and password to access the network behind the security appliance, even though the tunnel already exists.

Note You cannot use the command-line interface to log in if user authentication is enabled. You must use a browser.

If you have a default home page on the remote network behind the security appliance, or if you direct the browser to a website on the remote network behind the security appliance, the VPN 3002 directs the browser to the proper pages for user login. When you successfully log in, the browser displays the page you originally entered.

If you try to access resources on the network behind the security appliance that are not web-based, for example, e-mail, the connection fails until you authenticate using a browser.

To authenticate, you must enter the IP address for the private interface of the VPN 3002 in the browser Location or Address field. The browser then displays the login screen for the VPN 3002. To authenticate, click the Connect/Login Status button.

One user can log in for a maximum of four sessions simultaneously. Individual users authenticate according to the order of authentication servers that you configure for a group.

Configuring an Idle Timeout

To set an idle timeout for individual users behind hardware clients, clear the Inherit check box and either check the Unlimited check box to specify that there is no idle timeout or specify a specific number of minutes. If there is no communication activity by a user behind a hardware client in the idle timeout period, the security appliance terminates the client's access.

Note The **user-authentication-idle-timeout** command terminates only the client's access through the VPN tunnel, not the VPN tunnel itself.

The **minutes** field specifies the number of minutes in the idle timeout period.The minimum is 1 minute, the default is 30 minutes, and the maximum is 35791394 minutes. If you clear both the Inherit and Unlimited check boxes, you must specify a value in the minutes field.

Configuring IP Phone Bypass

You can allow Cisco IP phones to bypass individual user authentication behind a hardware client. To enable or disable IP Phone Bypass, clear the Inherit check box and select **Enable** or **Disable**. IP Phone Bypass lets IP phones behind hardware clients connect without undergoing user authentication processes. IP Phone Bypass is disabled by default. If enabled, secure unit authentication remains in effect.

Note You must configure the VPN 3002 to use network extension mode for IP phone connections.

Configuring LEAP Bypass

LEAP users behind a VPN 3002 have a circular dilemma: they cannot negotiate LEAP authentication because they cannot send their credentials to the RADIUS server behind the central site device over the tunnel. The reason they cannot send their credentials over the tunnel is that they have not authenticated on the wireless network. To solve this problem, LEAP Bypass lets LEAP packets, and only LEAP packets, traverse the tunnel to authenticate the wireless connection to a RADIUS server before individual users authenticate. Then the users proceed with individual user authentication.

LEAP Bypass works as intended under the following conditions:

- The interactive unit authentication feature (intended for wired devices) must be disabled. If interactive unit authentication is enabled, a non-LEAP (wired) device must authenticate the VPN 3002 before LEAP devices can connect using that tunnel.
- Individual user authentication is enabled (if it is not, you do not need LEAP Bypass).
- Access points in the wireless environment must be Cisco Aironet Access Points. The wireless NIC cards for PCs can be other brands.
- The Cisco Aironet Access Point must be running Cisco Discovery Protocol (CDP).
- The VPN 3002 can operate in either client mode or network extension mode.
- LEAP packets travel over the tunnel to a RADIUS server via ports 1645 or 1812.

When LEAP Bypass is enabled, LEAP packets from wireless devices behind a VPN 3002 hardware client travel across a VPN tunnel prior to user authentication. This action lets workstations using Cisco wireless access point devices establish LEAP authentication and then authenticate again per user authentication (if enabled). LEAP Bypass is disabled by default.

To allow LEAP packets from Cisco wireless access points to bypass individual users authentication, clear the Inherit check box and select **Enable**. To disable LEAP bypass, select **Disable**.

Note IEEE 802.1X is a standard for authentication on wired and wireless networks. It provides wireless LANs with strong mutual authentication between clients and authentication servers, which can provide dynamic per-user, per session wireless encryption privacy (WEP) keys, removing administrative burdens and security issues that are present with static WEP keys.

Cisco Systems has developed an 802.1X wireless authentication type called Cisco LEAP. LEAP (Lightweight Extensible Authentication Protocol) implements mutual authentication between a wireless client on one side of a connection and a RADIUS server on the other side. The credentials used for authentication, including a password, are always encrypted before they are transmitted over the wireless medium.

Cisco LEAP authenticates wireless clients to RADIUS servers. It does not include RADIUS accounting services.

This feature does not work as intended if you enable interactive hardware client authentication.

Caution There might be security risks to your network in allowing any unauthenticated traffic to traverse the tunnel.

Enabling Network Extension Mode

Network extension mode lets hardware clients present a single, routable network to the remote private network over the VPN tunnel. IPSec encapsulates all traffic from the private network behind the hardware client to networks behind the security appliance. PAT does not apply. Therefore, devices behind the security appliance have direct access to devices on the private network behind the hardware client over the tunnel, and only over the tunnel, and vice versa. The hardware client must initiate the tunnel, but after the tunnel is up, either side can initiate data exchange.

Network extension mode is required for the VPN 3002 to support IP phone connections, because the Call Manager can communicate only with actual IP addresses.

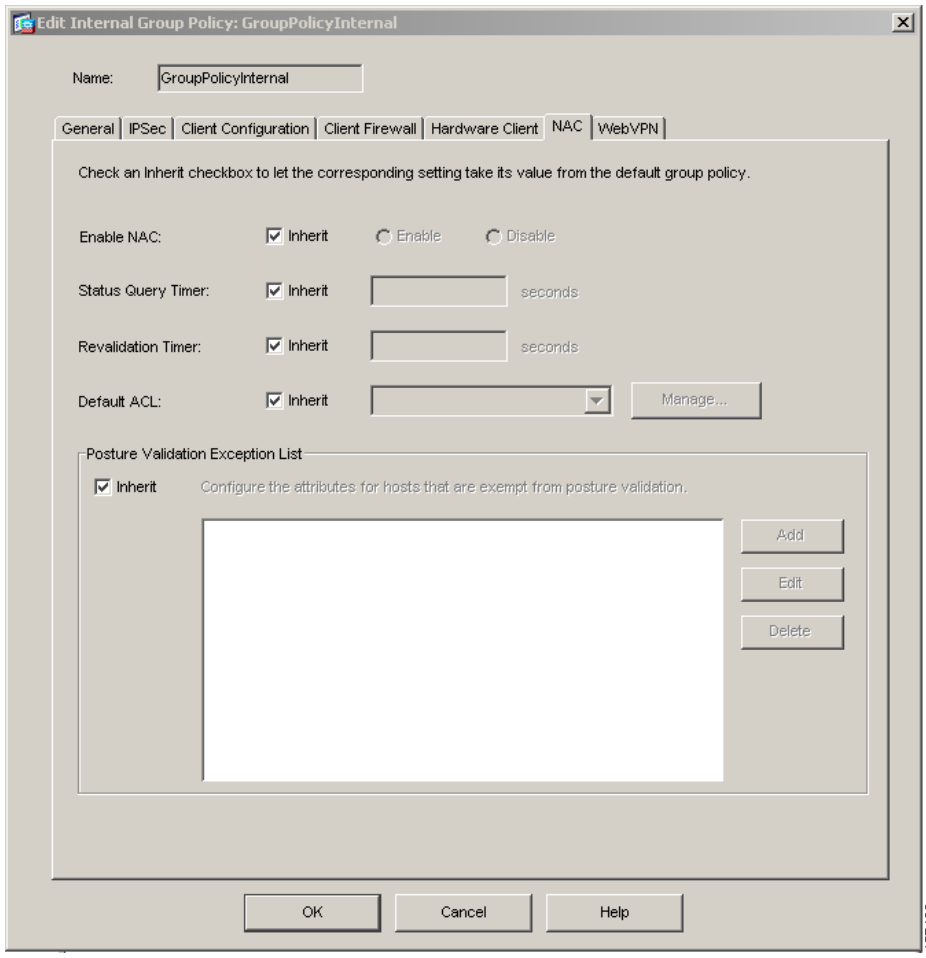
Note If you disallow network extension mode, the default setting, the VPN 3002 can connect to this security appliance in PAT mode only. If you disallow network extension mode here, be careful to configure all VPN 3002s in a group for PAT mode. If a VPN 3002 is configured to use network extension mode and the security appliance to which it connects disallows network extension mode, the VPN 3002 attempts to connect every 4 seconds, and every attempt is rejected. In this situation, the VPN 3002 puts an unnecessary processing load on the security appliance to which it connects; if large numbers of VPN 3002s are misconfigured in this way, the security appliance has a reduced ability to provide service.

Enable or disable network extension mode for hardware clients by clearing the Inherit check box and selecting **Enable** or **Disable**.

Configuring Network Admission Control

The Add or Edit Internal Group Policy window, NAC tab (Figure 2-33), lets you configure Network Admission Control settings for the default group policy or an alternative group policy.

Figure 2-33 NAC Tab



The default for all the parameters on this tab is to inherit the value from the default group policy. Clear the Inherit check box for any parameters you want to explicitly configure. The fields on this window are as follows:

- Inherit—(Multiple instances) Indicates that the corresponding setting takes its value from the default group policy, rather than from the explicit specifications that follow. This is the default setting for all attributes in this tab.
- Enable NAC—Requires posture validation for remote access. If the remote computer passes the validation checks, the ACS server downloads the access policy for the security appliance to enforce. The default setting is Disable.
- Status Query Timer—The security appliance starts this timer after each successful posture validation and status query response. The expiration of this timer triggers a query for changes in the host posture, referred to as a *status query*. Enter the number of seconds in the range 30 to 1800. The default setting is 300.
- Revalidation Timer—The security appliance starts this timer after each successful posture validation. The expiration of this timer triggers the next unconditional posture validation. The security appliance maintains posture validation during revalidation. The default group policy

becomes effective if the Access Control Server is unavailable during posture validation or revalidation. Enter the interval in seconds between each successful posture validation. The range is 300 to 86400. The default setting is 36000.

- Default ACL— (Optional) The security appliance applies the security policy associated with the selected ACL if posture validation fails. Select None or select an extended ACL in the list. The default setting is None. If the setting is None and posture validation fails, the security appliance applies the default group policy.

  Use the Manage button to populate the drop-down list and view the configuration of the ACLs in the list.
- Manage— Opens the ACL Manager dialog box. Click to view, enable, disable, and delete standard ACLs and the ACEs in each ACL. The list next to the Default ACL attribute displays the ACLs.
- Posture Validation Exception List—Displays one or more attributes that exempt remote computers from posture validation. At minimum, each entry lists the operating system and an Enabled setting of Yes or No. An optional filter identifies an ACL used to match additional attributes of the remote computer. An entry that consists of an operating system and a filter requires the remote computer to match both to be exempt from posture validation. The security appliance ignores the entry if the Enabled setting is set to No.
- Add—Adds an entry to the Posture Validation Exception list.
- Edit—Modifies an entry in the Posture Validation Exception list.
- Delete—Removes an entry from the Posture Validation Exception list.

Configuring Group-Policy WebVPN Attributes

WebVPN lets users establish a secure, remote-access VPN tunnel to the security appliance using a web browser. There is no need for either a software or hardware client. WebVPN provides easy access to a broad range of web resources and web-enabled applications from almost any computer that can reach HTTPS Internet sites. WebVPN uses SSL and its successor, TLS1, to provide a secure connection between remote users and specific, supported internal resources that you configure at a central site. The security appliance recognizes connections that need to be proxied, and the HTTP server interacts with the authentication subsystem to authenticate users. By default, WebVPN is disabled.

You can customize a WebVPN configuration for specific internal group policies.

In the Add or Edit Internal Group Policy WebVPN tab, you can specify whether to inherit the settings for all the functions or customize the WebVPN attributes, each of which is described in the subsequent sections:

- Functions
- Content Filtering
- Homepage
- Port Forwarding
- Other (such as servers and URL lists)
- SSL VPN Client (SVC)
- Auto Signon

In many instances, you define the WebVPN attributes as part of configuring WebVPN, then you apply those definitions to specific groups when you configure the group-policy webvpn attributes. The attributes in the WebVPN tab for group policies define access to files, MAPI proxy, URLs and TCP applications over WebVPN. They also identify ACLs and types of traffic to filter. WebVPN is disabled

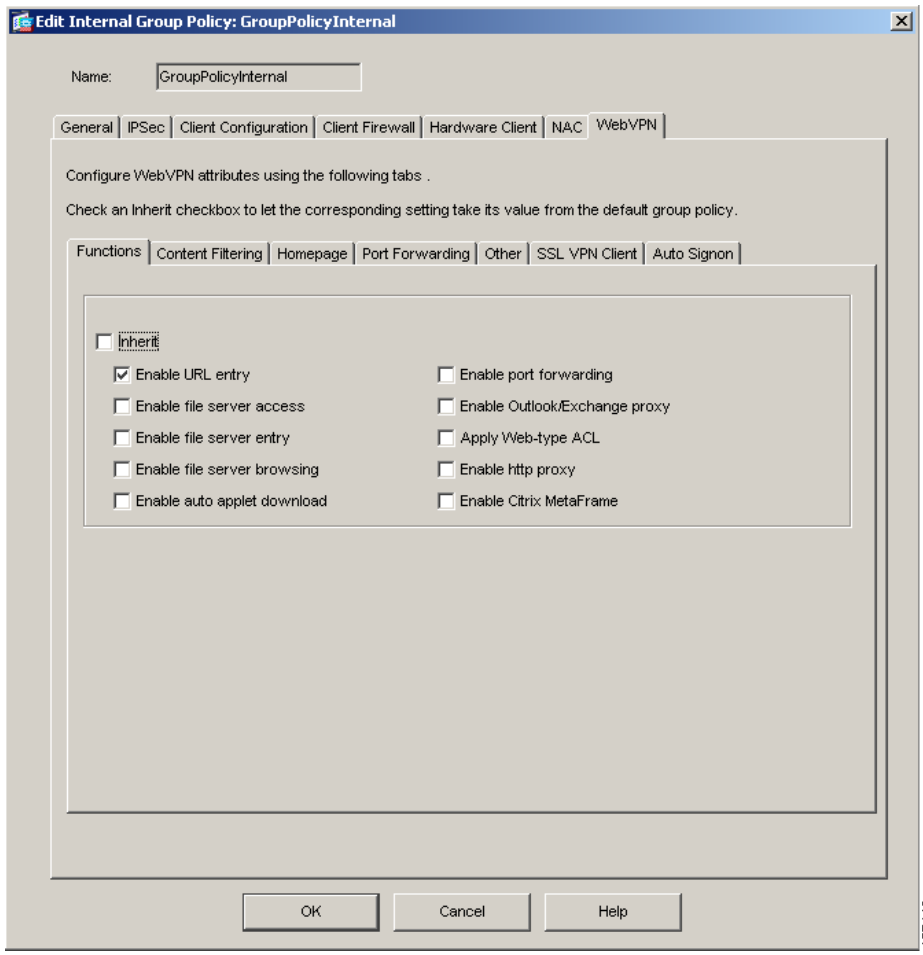
by default. See the description of WebVPN in the online Help for this tab and the *Cisco Security Appliance Command Line Configuration Guide* and *Cisco Security Appliance Command Reference* for more information about configuring the WebVPN attributes.

You do not need to configure WebVPN to use e-mail proxies.

Configuring Group-Policy WebVPN Function Tab Attributes

The Functions tab (Figure 2-34) lets you configure basic WebVPN functions. To configure the WebVPN functions (such as file access and file browsing, HTTP Proxy, MAPI Proxy, and URL entry over WebVPN) that you want to enable, clear the Inherit check box and check the check boxes for the individual functions that you want to enable or apply. These functions are disabled by default.

Figure 2-34 Edit Internal Group Policy WebVPN Tab Functions Tab



The functions that you can configure on this tab are as follows:

- Enable URL entry—Enables or disables user entry of URLs and places the URL entry box on the home page. When enabled, the security appliance still restricts URLs with any configured URL or network ACLs. Users can enter web addresses in the URL entry box, and use WebVPN to access those websites. When URL entry is disabled, the security appliance restricts WebVPN users to the URLs on the home page.

Using WebVPN does not ensure that communication with every site is secure. WebVPN ensures the security of data transmission between the remote user's PC or workstation and the security appliance on the corporate network. If a user then accesses a non-HTTPS web resource (located on the Internet or on the internal network), the communication from the corporate security appliance to the destination web server is not secured.

In a WebVPN connection, the security appliance acts as a proxy between the end user's web browser and target web servers. When a WebVPN user connects to an SSL-enabled web server, the security appliance establishes a secure connection and validates the server's SSL certificate. The end user's browser never receives the presented certificate, so therefore cannot examine and validate the certificate. The current implementation of WebVPN does not permit communication with sites that present expired certificates. Neither does the security appliance perform trusted CA certificate validation. Therefore, WebVPN users cannot analyze the certificate an SSL-enabled web-server presents before communicating with it.

To limit Internet access for WebVPN users, deselect the Enable URL Entry field. This prevents WebVPN users from surfing the Web during a WebVPN connection.

- Enable file server access—Enables or disables Windows file access (SMB/CIFS files only) through HTTPS. When enabled, the WebVPN home page lists file servers in the server list. You must enable file access to enable file browsing and/or file entry.

  When this box is checked, users can access Windows files on the network. If you enable only this parameter for WebVPN file sharing, users can access only servers that you configure in the Servers and URLs area (see the description of Configuring Server and List Arguments Using the WebVPN Other Tab, page 2-55). To let users access servers directly or to browse servers on the network, see the Enable file server entry and Enable file server browsing attribute descriptions.

  With this check box checked, users can download, edit, delete, rename, and move files. They can also add files and folders.

  Shares must also be configured for user access on the applicable Windows servers. Users might have to be authenticated before accessing files, depending on network requirements.

  File access, server/domain access, and browsing require that you configure a WINS server or a master browser, typically on the same network as the security appliance, or reachable from that network. The WINS server or master browser provides the security appliance with an list of the resources on the network. You cannot use a DNS server instead.

Note File access is not supported in an Active Native Directory environment when used with Dynamic DNS. It is supported if used with a WINS server.

- Enable file server entry—Enables of disables user ability to enter names of file servers. Places the file server entry box on the portal page. File server access must be enabled.

  With this check box checked, users can enter pathnames to directly Windows files. They can download, edit, delete, rename, and move files. They can also add files and folders. Again, shares must also be configured for user access on the applicable Windows servers. Users might have to be authenticated before accessing files, depending on network requirements.

- Enable file server browsing—Enables or disables browsing for file the Windows network for domains/workgroups, file servers and shares. You must enable file browsing to allow user entry of a file server. File server access must be enabled.

  With this check box checked, users can select domains and workgroups and can browse servers and shares within those domains. Shares must also be configured for user access on the applicable Windows servers. Users may need to be authenticated before accessing servers, according to network requirements.

- Enable auto applet download—Lets users automatically download and start the port forwarding java applet upon WebVPN login. Disabled by default, you can enable this feature only if port forwarding, Outlook/Exchange proxy, or HTTP proxy is also enabled. You can also enable auto applet download in the default group policy (DfltGrpPolicy) or in user-defined group policies.
- Enable port forwarding—WebVPN Port Forwarding provides access for remote users in the group to client/server applications that communicate over known, fixed TCP/IP ports. Remote users can use client applications that are installed on their local PC and securely access a remote server that supports that application. Cisco has tested the following applications: Windows Terminal Services, Telnet, Secure FTP (FTP over SSH), Perforce, Outlook Express, and Lotus Notes. Other TCP-based applications may also work, but Cisco has not tested them.

Note Port Forwarding does not work with some SSL/TLS versions.

With this check box checked users can access client/server applications by mapping TCP ports on the local and remote systems.

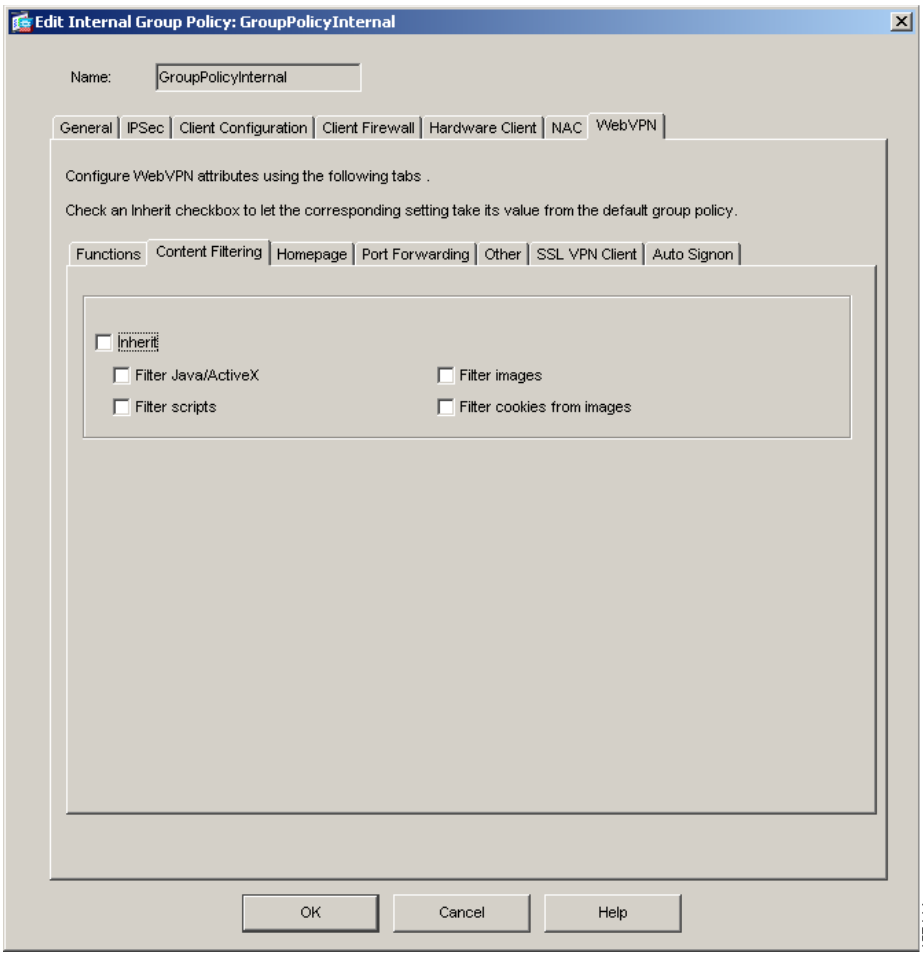
Note When users authenticate using digital certificates, the TCP Port Forwarding JAVA applet does not work. JAVA cannot access the web browser's keystore; therefore JAVA cannot use the certificates that the browser uses for user authentication, and the application cannot start. Do not use digital certificates to authenticate WebVPN users if you want them to be able to access applications.

- Enable Outlook/Exchange proxy—Enables or disables Microsoft Outlook/Exchange e-mail proxy.
- Apply Web-type ACL—Applies the WebVPN access control list defined for the users of this group.
- Enable HTTP proxy—Enables or disables the forwarding of an HTTP applet proxy to the client. The proxy is useful for technologies that interfere with proper content transformation (“mangling”), such as Java, ActiveX, and Flash. It bypasses mangling while ensuring the continued use of the security appliance. The forwarded proxy modifies the browser’s old proxy configuration automatically and redirects all HTTP and HTTPS requests to the new proxy configuration. It supports virtually all client side technologies, including HTML, CSS, JavaScript, VBScript, ActiveX, and Java. The only browser supported is Microsoft Internet Explorer.
- Enable Citrix/MetaFrame—Enables support for terminal services from a MetaFrame Application Server to the client. This attribute lets the security appliance act as a secure gateway within a secure Citrix configuration. These services provide users with access to MetaFrame applications through a standard Web browser.

Configuring Content Filtering Tab Attributes

The Content Filtering tab (Figure 2-35) lets you configure the security appliance to block or remove the parts of websites that use Java or Active X, scripts, display images, and deliver cookies. By default, these parameters are disabled, which means that no filtering occurs. To configure the WebVPN filters, clear the Inherit check box and check the check boxes for the individual filters that you want to enable. These functions are disabled by default.

Figure 2-35 Edit Internal Group Policy WebVPN Tab, Content Filtering Tab



The filters that you can configure on this tab are as follows:

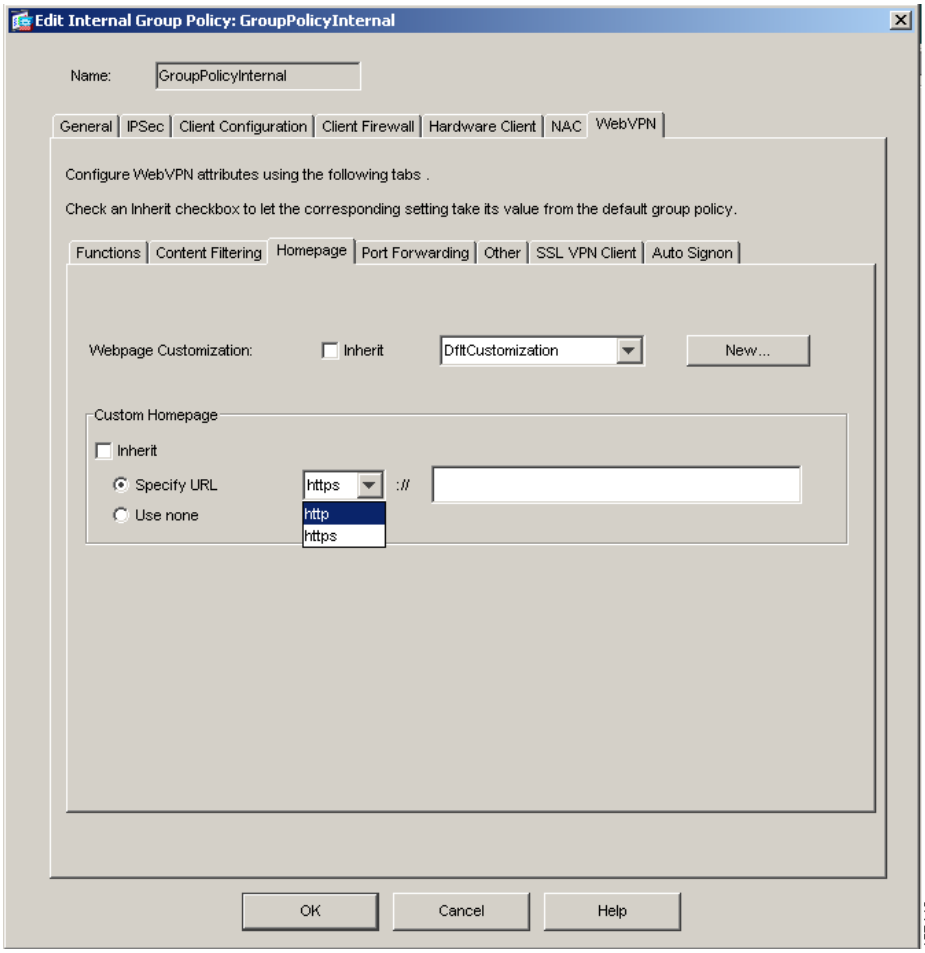
- Filter Java/ActiveX—Removes references to Java and ActiveX; that is, it removes <applet>, <embed> and <object> tags from HTML.
- Filter scripts—Removes references to scripting; that is, it removes <script> tags from HTML.
- Filter images—Removes <img> tags from HTML. Removing images dramatically speeds the delivery of web pages.
- Filter cookies from images—Removes cookies that are delivered with images. This might preserve user privacy, because advertisers use cookies to track visitors.

Configuring the User Homepage

ASDM lets you customize a home page that the user sees upon logging in. You define a home page customization (such as color, logo, and so on) as part of the WebVPN configuration, then apply that customization when you configure a particular group policy. The Add or Edit Group Policy window, WebVPN tab, Homepage tab (Figure 2-36), lets you configure what, if any, home page that you want users to see upon logging in and specify the name of any previously defined customization that you want

to apply to change the look-and-feel of that login web page. There is no default home page, and the default for customization is no customization. For information about configuring web-page customizations, see the online help for Configuration > VPN > WebVPN > Webpage Customization.

Figure 2-36 Edit Internal Group Policy WebVPN Tab Homepage Tab



To specify the Webpage Customization attribute, clear the Inherit check box and either select the name of a customization from the drop-down menu or click **New** to define a new customization. Clicking **New** opens the Add Customization Object dialog box. Click the **Homepage** tab in that dialog box to configure the customizations for the user home page. The other tabs in this dialog box configure other web page customizations to apply to the various GUI pages that the user sees. For information about how to configure web page customizations, see the online Help for that dialog box.

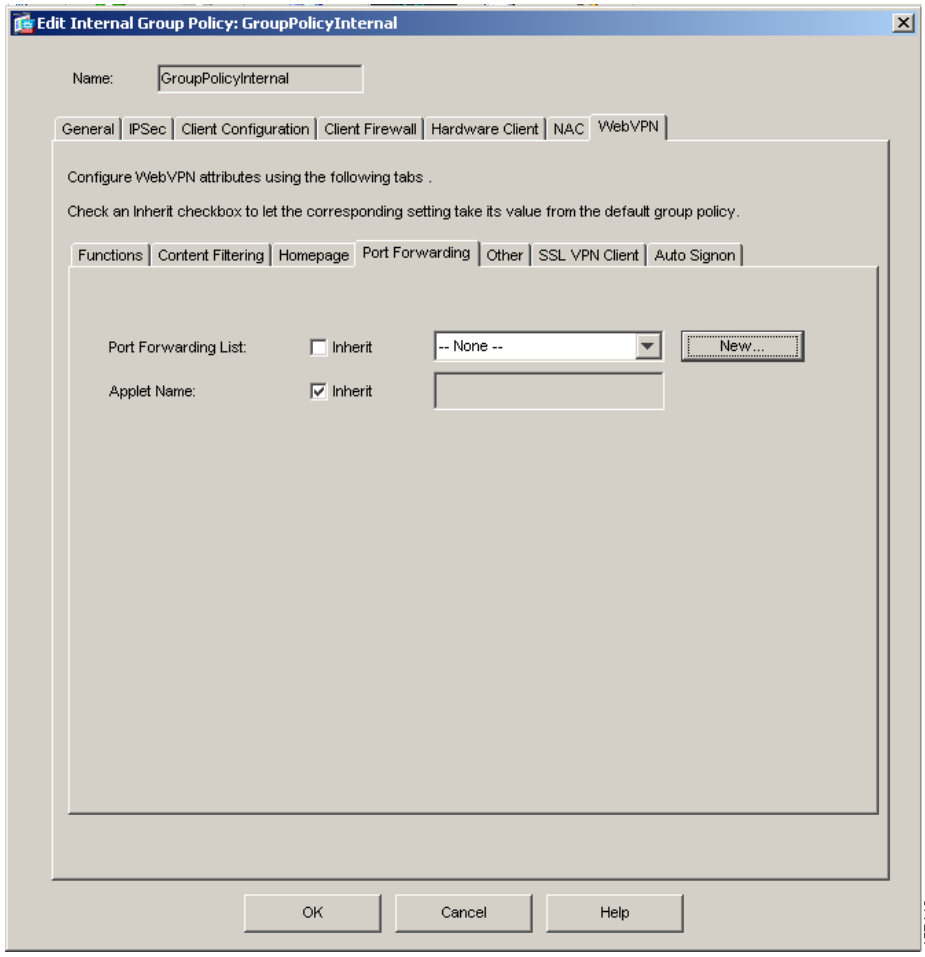
Regardless of whether you specify customizations, you can specify a particular home page that the user sees upon logging in. There is no default home page. To specify a URL for the web page that you want to display when a user in this group logs in, clear the Inherit check box in the Custom Homepage area and select **Specify URL**. Select either **http** or **https** (the default) as http or https as the connection protocol for the home page. In the field to the right of the :// characters, specify the URL of the Web page to use as the home page.

To remove a configured home page, select **Use None**. This sets a null value, thereby disallowing a home page and prevents inheriting an home page.

Enabling Port Forwarding (WebVPN Application Access) for a Group Policy

Port forwarding, also known as application access, lets you control the list of applications that WebVPN users can access through their remote connection. Port forwarding is disabled by default. The Add or Edit Group Policy window, WebVPN tab, Port Forwarding tab (Figure 2-37), lets you configure port forwarding parameters.

Figure 2-37 Edit Internal Group Policy WebVPN Tab Port Forwarding Tab



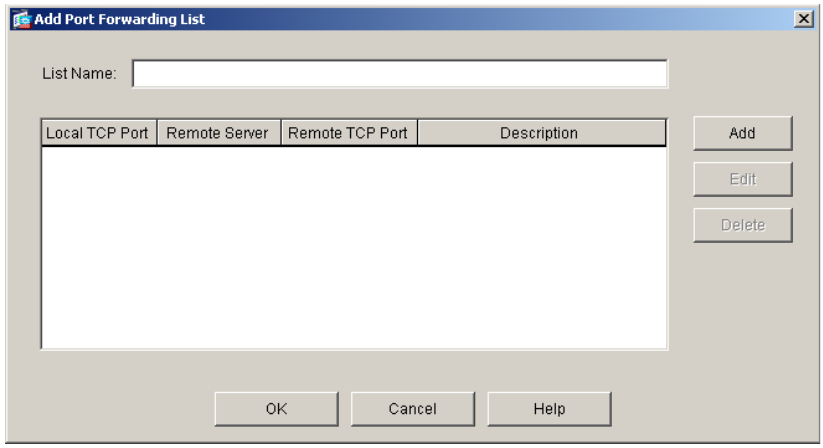
You configure a list of applications to make available through port forwarding either as part of the WebVPN configuration or in the group-policy Port Forwarding tab. To apply port forwarding to a group policy, clear the Inherit check box or boxes and configure the following fields:

- Port Forwarding List—Specifies whether to inherit the port forwarding list from the default group policy, select one from the list, or create a new port forwarding list. The default is **None**, which prevents inheriting a port forwarding list.
- Click **New** to create a new port-forwarding applications list. Clicking New opens a dialog box in which you can add a new port forwarding list. See the description of the Add or Edit Port Forwarding List window.

- Applet Name—Specifies whether to inherit the applet name or to use the name specified in the field. Specify this name to identify port forwarding to end users. The name you configure appears in the end user interface as a hotlink. When users click this link, a Java applet opens a window that displays a table that lists and provides access to port forwarding applications that you configure for these users. The default applet name is Application Access.

The Add or Edit Port Forwarding List dialog box (Figure 2-38) lets you configure a new port forwarding list entry or modify an existing entry for WebVPN users for the group policy being added or modified.

Figure 2-38 Add Port Forwarding List Dialog Box



To add a port forwarding list, click **Add** and configure the following fields. To edit an existing port forwarding list, select the list entry in the table area, then click **Edit** and configure the appropriate fields. To remove a port forwarding entry from this list, click **Delete**. The field descriptions follow:

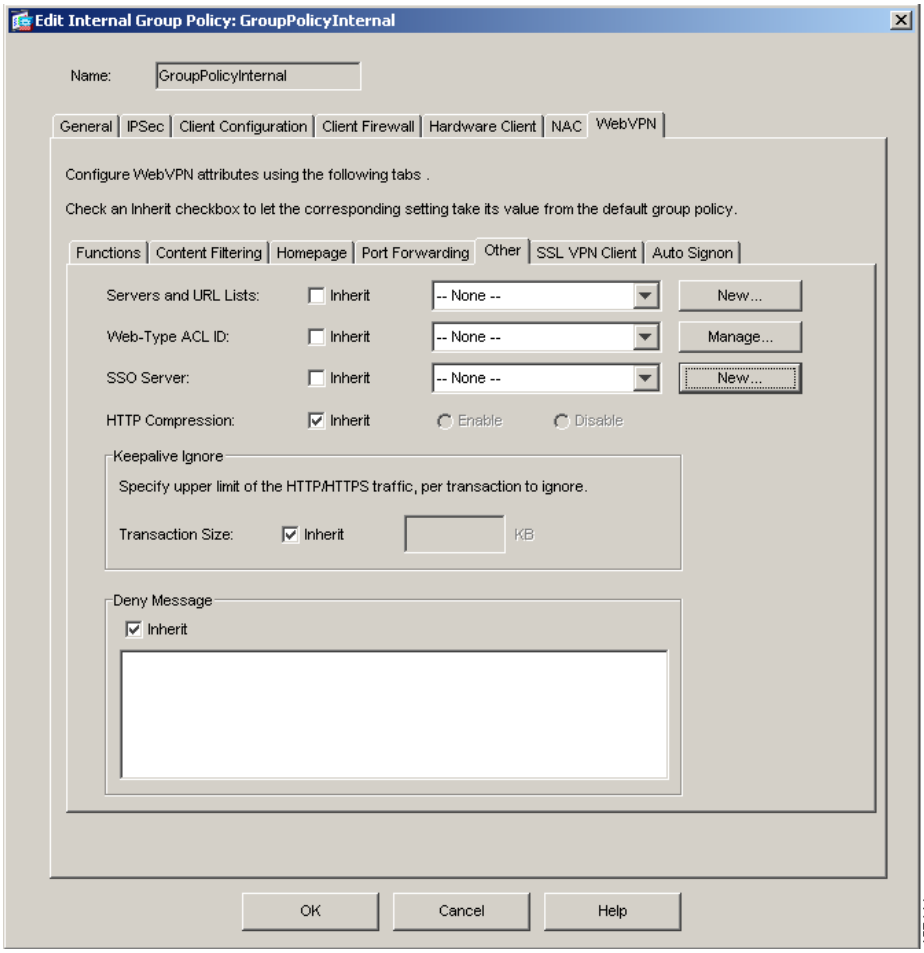
- List Name—Specifies the name of this port forwarding list. If list entries already exist, the Add, Edit, and Delete buttons are active. The table below the list name contains the following columns:
- Local TCP Port—Specifies the local TCP port for this list.
- Remote Server—Specifies the name or IP address of the remote peer.
- Remote TCP Port—Specifies the TCP port used on the remote peer.
- Description—Provides a brief description of this list.

Note Port forwarding supports only those TCP applications that use static TCP ports. It does not support applications that use dynamic ports or multiple TCP ports. For example, SecureFTP, which uses port 22, works over WebVPN port forwarding, but standard FTP, which uses ports 20 and 21, does not.

Configuring Server and List Arguments Using the WebVPN Other Tab

The Add or Edit Group Policy window, WebVPN tab, Other tab (Figure 2-39), lets you configure servers and URL lists and the Web-type ACL ID.

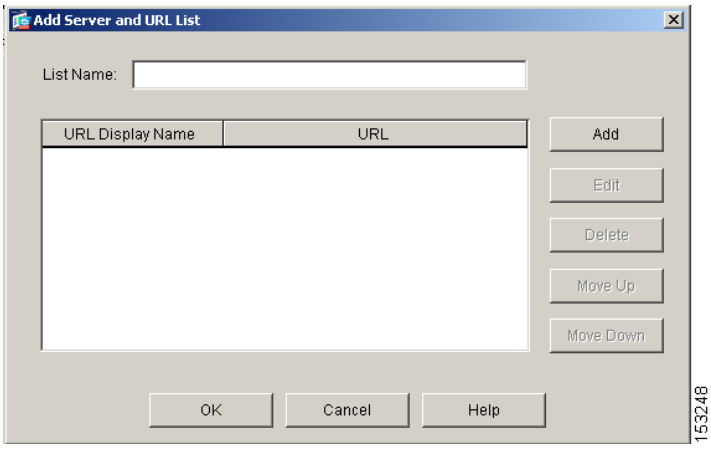
Figure 2-39 Edit Internal Group Policy WebVPN Tab Other Tab



This tab lets you configure an assortment of server and management functions, as follows. To configure individual fields, clear the Inherit check box for that field.

- Servers and URL Lists specifies whether to inherit the list of Servers and URLs, to select an existing list, or to create a new list. Select the name of a list from the drop-down menu or click **New**, which opens the Add Server and URL List dialog box (Figure 2-40), in which you can add a new server or URL to the list. The URL display name that you add in this dialog box appears in the list for the Servers and URL Lists argument in the Add or Edit Internal Group Policy WebVPN tab Other tab window. To change the order of entries in the URL list, click **Move Up** or **Move Down**. There is no default URL list.

Figure 2-40 Add Server and URL List Dialog Box



- You configure ACLs to permit or deny various types of traffic for this group policy. You then *apply* those ACLs for WebVPN traffic. Web-Type ACL ID specifies the name of the access list to apply for WebVPN connections for this group policy. If you clear the Inherit check box, select the identifier of an existing Web-Type ACL to use, or add or modify a web-type ACL. To remove the access list, and to prevent inheriting filter values, select **None** from the drop-down list.
- Clicking Manage opens the Web Type ACL dialog box (Figure 2-9) in which you can manage web-type ACLs.

  Clicking Add ACL, Add ACE, or Edit ACE opens a dialog box in which you can perform these functions. See Configuring the ACL Filter, page 2-12 for an explanation of the fields and buttons on these dialog boxes.

  After you add a Web Type ACL, you can configure that ACL by clicking Add ACE. This opens the Add ACE dialog box, in which you configure the action (permit/deny), filter (URL or IP address, subnet mask, and port), syslog options, and time range name, just as you would for other ACLs/ACEs.

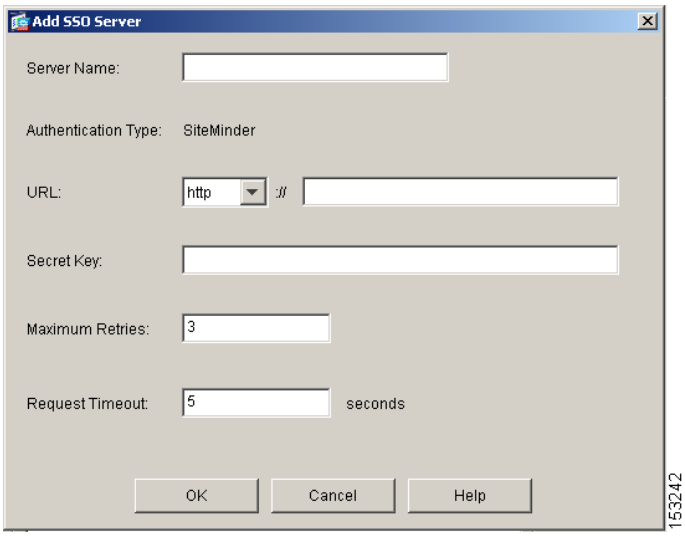
Note To use ACL filtering with WebVPN, you must define the WebVPN-Type ACL here. WebVPN does not use ACLs defined in the ACL Manager.

- The **SSO Server** attribute specifies whether to inherit the single-sign-on server setting, to select an existing SSO server from the list, or to add a new SSO server.Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. The default policy assigned to the SSO server is DfltGrpPolicy. To remove the assignment and prevent inheriting the default policy, select **None** from the drop-down list.

Note This attribute requires that your configuration include CA SiteMinder.

Click **New** to open the Add SSO Server dialog box (Figure 2-41) in which you can add a new server to the list.

Figure 2-41 Add SSO Server



Configure the fields in this dialog box as follows:

- Specify the name of the server in the Server Name field. This name appears in the drop-down menu for the SSO Server attribute in the Add or Edit Internal Group Policy WebVPN tab Other tab. If you are editing, instead of adding, a server, this field is display only; it displays the name of the selected SSO server.
- The Authentication Type field is display only. It displays the type of SSO server. The type currently supported by the security appliance is SiteMinder.
- In the URL field, select the protocol (http or https) from the drop-down menu, then enter the SSO server URL to which the security appliance makes SSO authentication requests.
- Enter a Secret Key to use to encrypt authentication requests to the SSO server. Key characters can be any regular or shifted alphanumeric characters. There is no minimum or maximum number of characters. The secret key is similar to a password: you create it, save it, and configure it. It is configured on both the security appliance and the SiteMinder Policy Server using the Cisco Java plug-in authentication scheme.
- In the Maximum Retries field, enter the number of times the security appliance retries a failed SSO authentication attempt before the authentication times-out. The range is from 1 to 5 retries inclusive, and the default is 3 retries.
- In the Request Timeout field, enter the number of seconds before a failed SSO authentication attempt times out. The range is from1 to 30 seconds inclusive, and the default is 5 seconds.

- HTTP Compression specifies whether to inherit the HTTP Compression setting from the default group, or explicitly to enable or disable HTTP compression. To enable or disable compression of HTTP data over an SVC connection for a specific group policy, clear the Inherit check box and select Enable or Disable, as appropriate. By default, SVC compression is enabled.
- Network devices exchange short keepalive messages to ensure that the virtual circuit between them is still active. The length of these messages can vary. The Keepalive Ignore attribute lets you tell the security appliance to consider all messages that are less than or equal to the specified size as keepalive messages and not as traffic when updating the session timer. The range is 0 through 900 KB. The default is 4 KB.
- The Deny Message attribute configures a message to be delivered to remote users who log in to WebVPN successfully, but have no VPN privileges, as follows:

- Check the Inherit check box to inherit from the default group the message to be sent to remote users who log in to WebVPN successfully, but have no VPN privileges.
- Clear the Inherit check box and erase any text in the field, to *not* send a message to remote users who log into WebVPN successfully, but have no VPN privileges.
- Clear the Inherit check box and create or modify the message in the field, to be sent to remote users who log in to WebVPN successfully, but have no VPN privileges. The message can be up to 491 alphanumeric characters long, including special characters, spaces, and punctuation, but not counting the enclosing quotation marks. Carriage return/line feeds count as two characters. The text appears on the remote user's browser upon login. The default deny message is: "Login was successful, but because certain criteria have not been met or due to some specific group policy, you do not have permission to use any of the VPN features. Contact your IT administrator for more information."

Configuring the SSL VPN Client Tab Attributes

The SSL VPN Client (SVC) is a VPN tunneling technology that gives remote users the benefits of an IPSec VPN client without the need for network administrators to install and configure IPSec VPN clients on remote computers. The SVC uses the SSL encryption that is already present on the remote computer as well as the WebVPN login and authentication of the security appliance.

To establish an SVC session, the remote user enters the IP address of a WebVPN interface of the security appliance in the browser, and the browser connects to that interface and displays the WebVPN login screen. If the user satisfies the login and authentication, and the security appliance identifies the user as *requiring* the SVC, the security appliance downloads the SVC to the remote computer. If the security appliance identifies the user as having the *option* to use the SVC, the security appliance downloads the SVC to the remote computer while presenting a link on the user screen to skip the SVC installation.

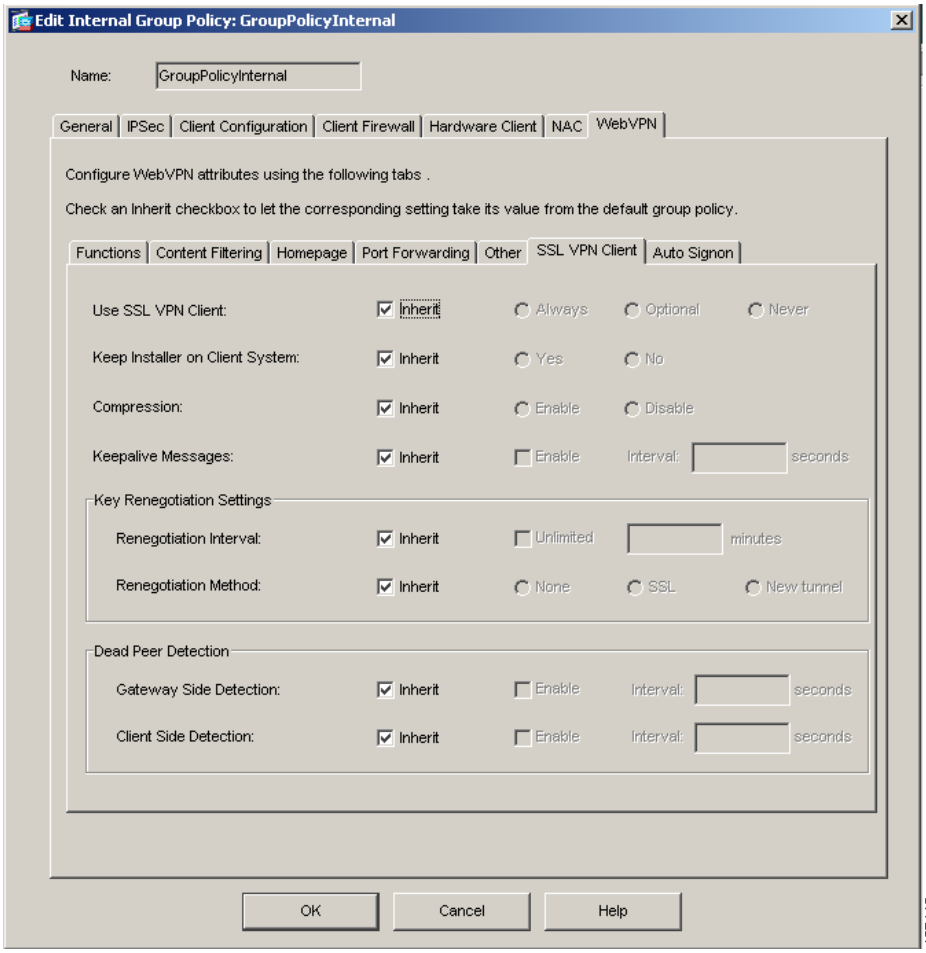
After downloading, the SVC installs and configures itself, and then the SVC either remains or uninstalls itself (depending on the configuration) from the remote computer when the connection terminates.

The security appliance might have several unique SVC images residing in cache memory for different remote computer operating systems. When the user attempts to connect, the security appliance can consecutively download portions of these images to the remote computer until the image and operating system match, at which point it downloads the entire SVC. You can order the SVC images to minimize connection setup time, with the first image downloaded representing the most commonly-encountered remote computer operating system. For complete information about installing and using SVC, see *Cisco Security Appliance Command Line Configuration Guide*, Chapter 31, "Configuring SSL VPN Client."

After enabling SVC, as described in that configuration guide chapter, you can enable or require SVC features for a specific group. This feature is disabled by default. If you enable or require SVC, you can then enable a succession of svc commands, described in this section.

The Edit Internal Group Policy window WebVPN tab SSL VPN tab (Figure 2-42) lets you configure connection settings for the SSL VPN Client. Each attribute can inherit its value from the default group policy, or, if you clear the Inherit check box, you can explicitly configure individual attributes.

Figure 2-42 Edit Internal Group Policy WebVPN Tab SSL VPN Client Tab



Configure the SSL VPN Client attributes as follows:

- Specify when to use the SSL VPN client by clearing the Use SSL VPN Client Inherit check box and selecting Always, Optional, or Never, as appropriate.
- Keep Installer on Client System enables permanent SVC installation and disables the automatic uninstalling feature of the SVC. If you select **Yes**, the security appliance downloads SVC files to remote computers, and the SVC remains installed on the remote computer for subsequent SVC connections, reducing the SVC connection time for the remote user. If you select No, the security appliance does not download SVC files. By default, this attribute is disabled.
- Compression enables or disables compression on the SVC connection. SVC compression increases the communications performance between the security appliance and the SVC by reducing the size of the packets being transferred.
- The Keepalive Messages attribute adjusts the frequency of keepalive messages, in the range of 15 to 600 seconds, to ensure that an SVC connection through a proxy, firewall, or NAT device remains open, even if the device limits the time that the connection can be idle. Clicking Enable activates the Interval field. You can adjust the interval (frequency) of keepalive messages to ensure that an SVC connection through a proxy, firewall, or NAT device remains open, even if the device limits the time

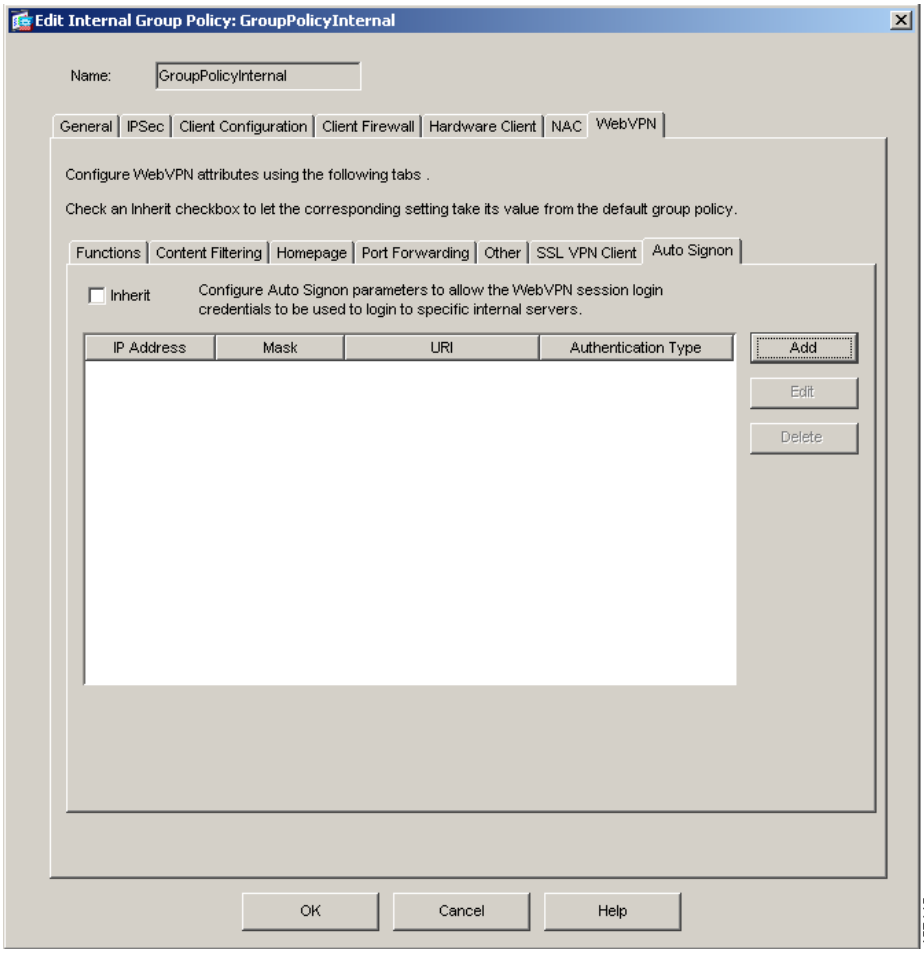
that the connection can be idle. Adjusting the frequency also ensures that the SVC does not disconnect and reconnect when the remote user is not actively running a socket-based application, such as Microsoft Outlook or Microsoft Internet Explorer.

- The attributes in the Key Renegotiation Settings area define the renegotiation interval and method. When the security appliance and the SVC perform a rekey, they renegotiate the crypto keys and initialization vectors, increasing the security of the connection.
  - Renegotiation Interval specifies the number of minutes from the start of the session until the rekey takes place, either Unlimited or an interval from 1 through 10080 (1 week).
  - Renegotiation Method specifies whether the SVC establishes a new tunnel during SVC rekey. Selecting None disables SVC rekey. Selecting SSL means that SSL renegotiation takes place during SVC rekey. Selecting New tunnel specifies that SVC creates a new VPN tunnel during SVC rekey.
- The attributes in the Dead Peer Detection (DPD) area ensure that the security appliance (gateway) or the SVC can quickly detect a condition where the peer is not responding, and the connection has failed. The attribute you select in this area determines which side of the connection performs DPD. For either of the following attributes, clearing the Inherit check box and the Enable check box and leaving the Interval field blank disables the attribute.
  - Gateway Side Detection enables DPD performed by the security appliance (gateway) and specifies the frequency, from 30 to 3600 seconds (1 hour), with which the security appliance performs DPD. If you check disable, DPD performed by the security appliance is disabled.
  - Client Side Detection enables DPD performed by the SVC (client), and specifies the frequency, from 30 to 3600 seconds (1 hour), with which the SVC performs DPD.

Configuring the Auto Signon Tab Attributes

The Auto Signon WebVPN tab (Figure 2-43) lets you configure or edit auto signon for WebVPN users.

Figure 2-43 WebVPN Auto Signon Tab

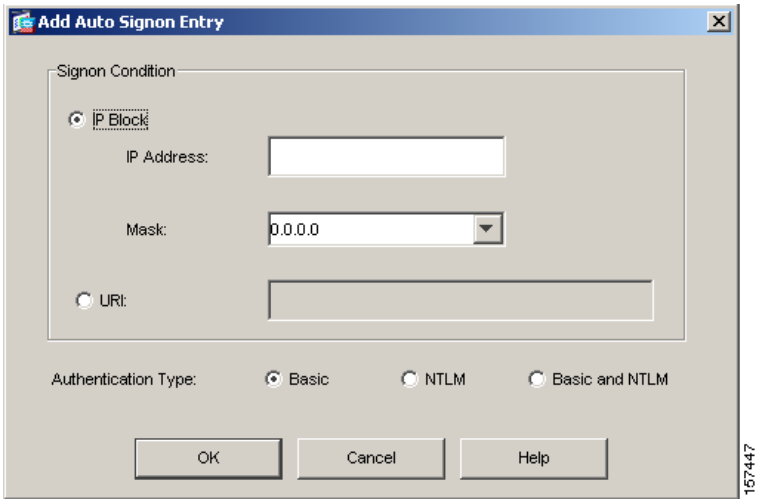


Auto signon is a simplified single signon method that you can use if you do not already have an SSO method deployed on your internal network. you already have SSO deployed using Computer Associates' SiteMinder SSO server.

You can also have SSO deployed using Computer Associates' SiteMinder SSO server and configure the security appliance to support this solution. You can use SSO with HTTP Forms protocol and configure the security appliance to support this method. With auto signon configured for particular internal servers, the security appliance passes the login credentials that the WebVPN user used to login to the security appliance (username and password) to those particular internal servers. You configure the security appliance to respond to a specific authentication method for a particular range of servers. The authentication methods you can configure the security appliance to respond to are NTLM authentication, HTTP Basic authentication, or both methods.

This section describes the procedure for setting up SSO with auto signon. Except for the Inherit check box, the fields on the Auto Signon tab are identical with those on the Add or Edit Auto Signon Entry dialog box (Figure 2-44).

Figure 2-44 Add Auto Signon Entry Dialog Box



Use the following descriptions when configuring or modifying the fields of an Auto Signon entry:

- Inherit—(Auto Signon tab only) Clear the check box to allow WebVPN login credentials to be used to login to specific internal servers.
- IP Address—In conjunction with the following Mask, displays the IP address range of the servers to be authenticated to as configured with the Add/Edit Auto Signon dialog box. You can specify a server using either the server URI or the server IP address and mask.
- Mask—In conjunction with the preceding IP Address, displays the IP address range of the servers configured to support auto signon with the Add/Edit Auto Signon dialog box.
- URI—Displays a URI mask that identifies the servers configured with the Add/Edit Auto Signon dialog box.
- Authentication Type— Displays the type of authentication—basic HTTP, NTLM, or basic and NTLM—as configured with the Add/Edit Auto Signon dialog box.
- Add/Edit—(Auto Signon tab only) Click to add or edit an auto signon instruction. An auto signon instruction defines a range of internal servers using the auto signon feature and the particular authentication method.
- Delete—(Auto Signon tab only) Click to delete an auto signon instruction selected in the Auto Signon table.

You have now completed the configuration of an internal group policy.

CHAPTER 3

Configuring the SSL VPN Client

The SSL VPN Client (SVC) is a VPN tunneling technology that gives remote users the benefits of an IPSec VPN client without the need for network administrators to install and configure IPSec VPN clients on remote computers. The SVC uses the SSL encryption that is already present on the remote computer as well as the WebVPN login and authentication of the security appliance.

To establish an SVC session, the remote user enters the IP address of a WebVPN interface of the security appliance in the browser, and the browser connects to that interface and displays the WebVPN login window. If the user satisfies the login and authentication, and the security appliance identifies the user as *requiring* the SVC, the security appliance downloads the SVC to the remote computer. If the security appliance identifies the user as having the *option* to use the SVC, the security appliance downloads the SVC to the remote computer while presenting a link on the window to skip the SVC installation.

After downloading, the SVC installs and configures itself, and then the SVC either remains or uninstalls itself (depending on the configuration) from the remote computer when the connection terminates.

This section covers the following topics:

Installing SVC

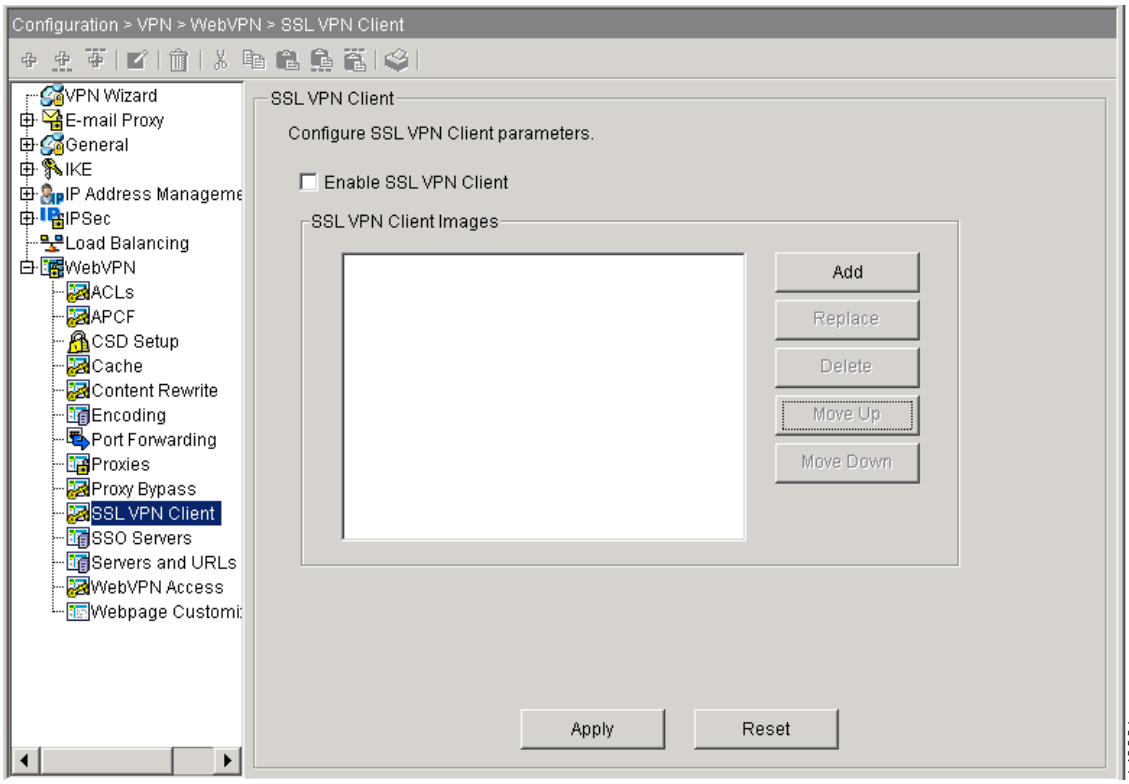
Installing SVC consists of uploading the SVC images to the flash memory, identifying to the security appliance the files on the flash memory to be used as SVC images, and setting the order in which it downloads the images to the remote computer.

Perform the following steps to install SVC:

Step 1 Upload the SVC images to the security appliance. On the ASDM toolbar, Select **Configuration > VPN > WebVPN > SSL VPN Client**. The SSL VPN Client panel appears. (Figure 3-1).

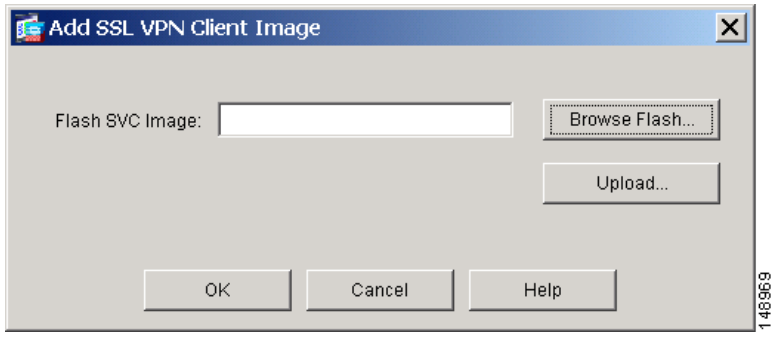
This window lists any SVC files that have been identified as SVC images. The order in which they appear in the table reflects the order that they download to the remote computer.

Figure 3-1 SSL VPN Client Window



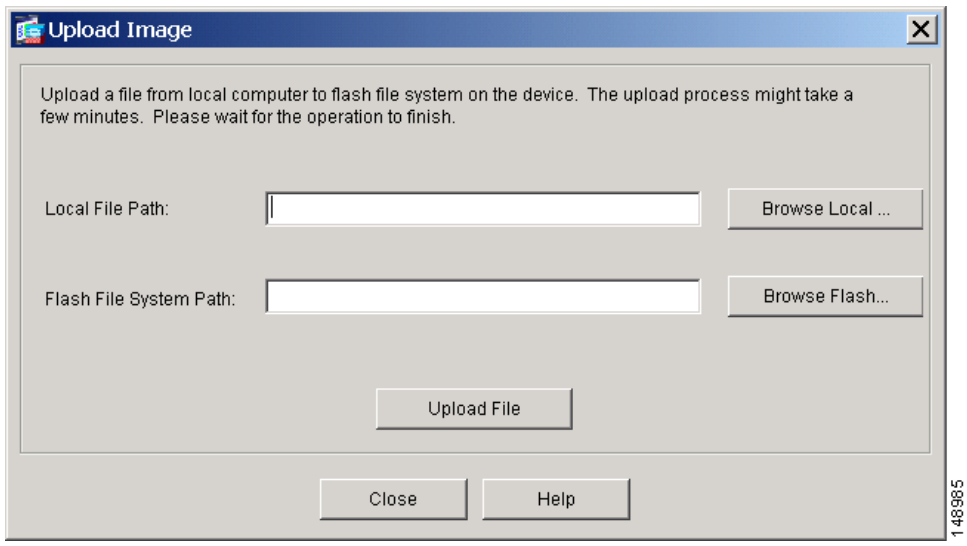
To add an SVC image, Click **Add**. The Add SSL VPN Client Image dialog box appears (Figure 3-2).

Figure 3-2 Add SSL VPN Client Image Dialog



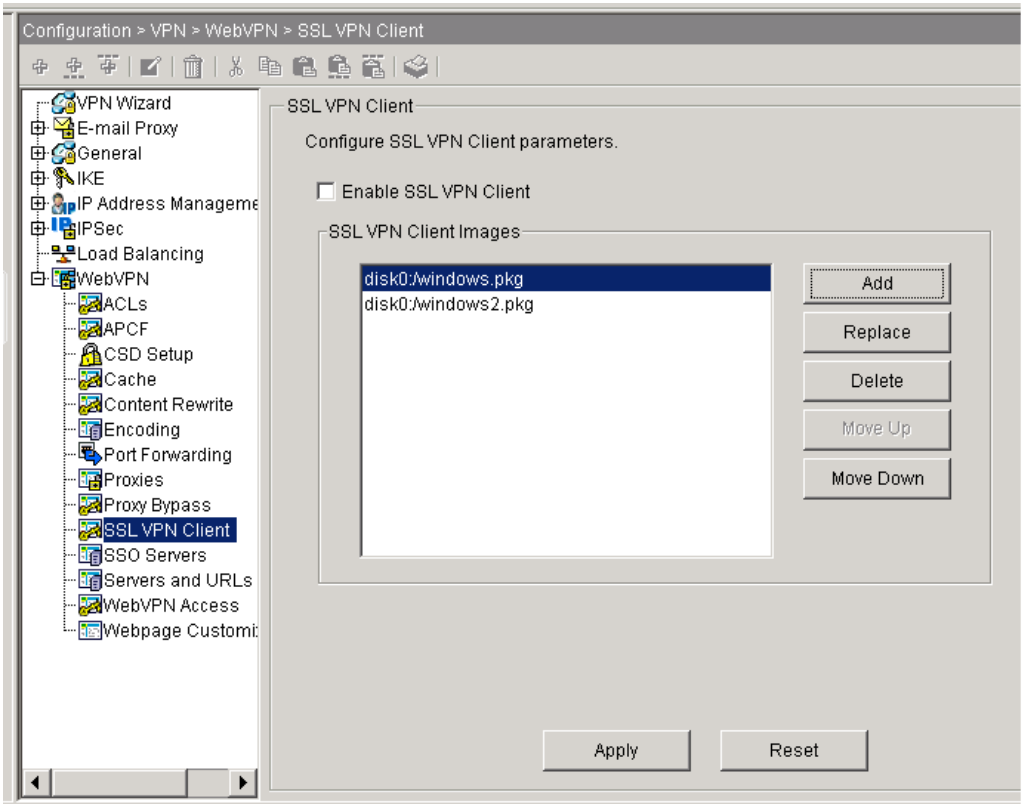
If you already have an image located in the flash memory of the security appliance, you can enter the name of the image in the Flash SVC Image field, and click **OK**. Otherwise, click **Upload** to browse the computer that is running ASDM. The Upload Image dialog box appears (Figure 3-3).

Figure 3-3 Upload Image Dialog



Enter the paths for the Local File Path and the Flash File System Path, or browse for the paths, and click **Upload File**. The SSL VPN Client window now shows the SVC images you identified (Figure 3-4).

Figure 3-4 SSL VPN Client Window with SVC Images

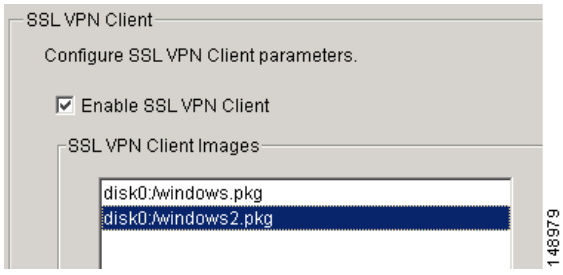


Step 2 Click on an image name, and use the **Move Down** button to change the position of the image within the list.

This establishes the order in which the security appliance downloads them to the remote computer. It downloads the SVC image at the top of the list of images first. Therefore, you should move the image used by the most commonly-encountered operating system to the top of the list.

Step 3 Check the **Enable SSL VPN Client** check box to enable the security appliance to download the SVC image(s) (Figure 3-5).

Figure 3-5 Enable SSL VPN Client Check Box

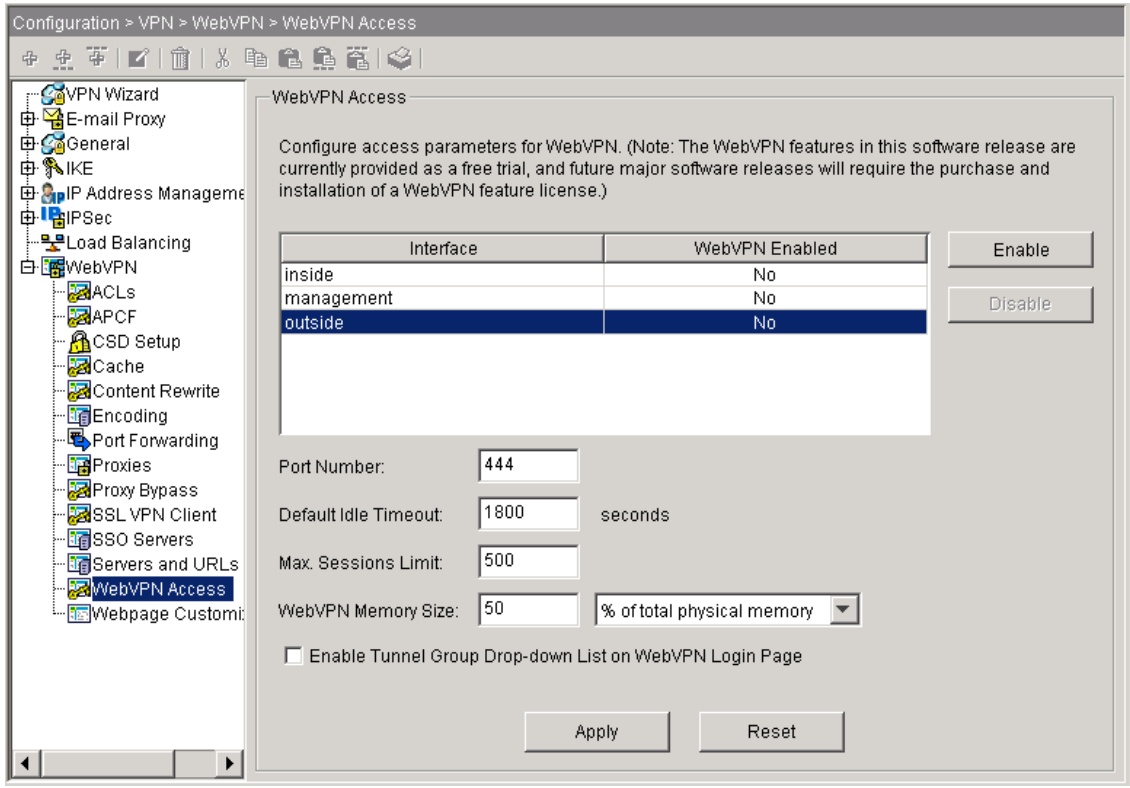


Configuring SVC

To configure SVC, perform the following steps:

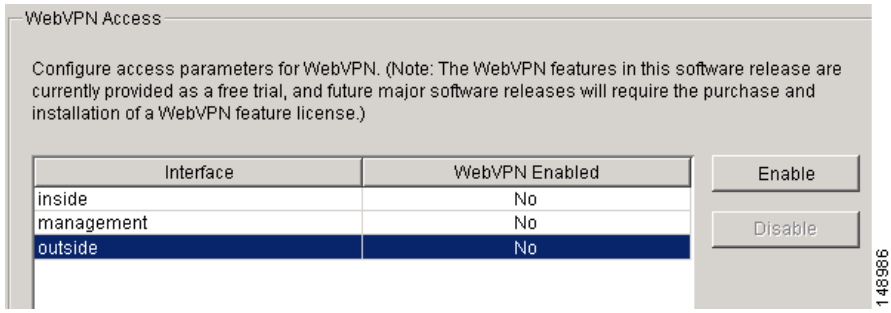
Step 1 Enable WebVPN on an interface. From the navigation pane, choose **WebVPN Access**. The WebVPN Access window appears (Figure 3-6).

Figure 3-6 WebVPN Access Window



Highlight an interface and click **Enable** (Figure 3-7).

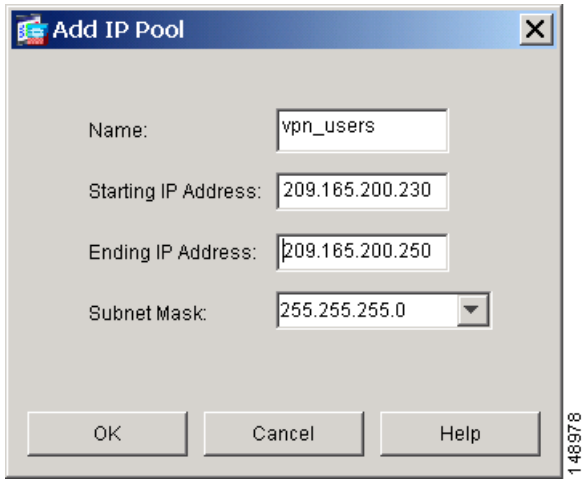
Figure 3-7 Enabling the Interface



Step 2 Configure a method of address assignment. You can use DHCP, and/or user-assigned addressing. You can also create a local IP address pool and assign the pool to a tunnel group.

To create an IP address pool, choose **Configuration > VPN > IP Address Management > IP Pools**. Click **Add**. The Add IP Pool dialog appears (Figure 3-8).

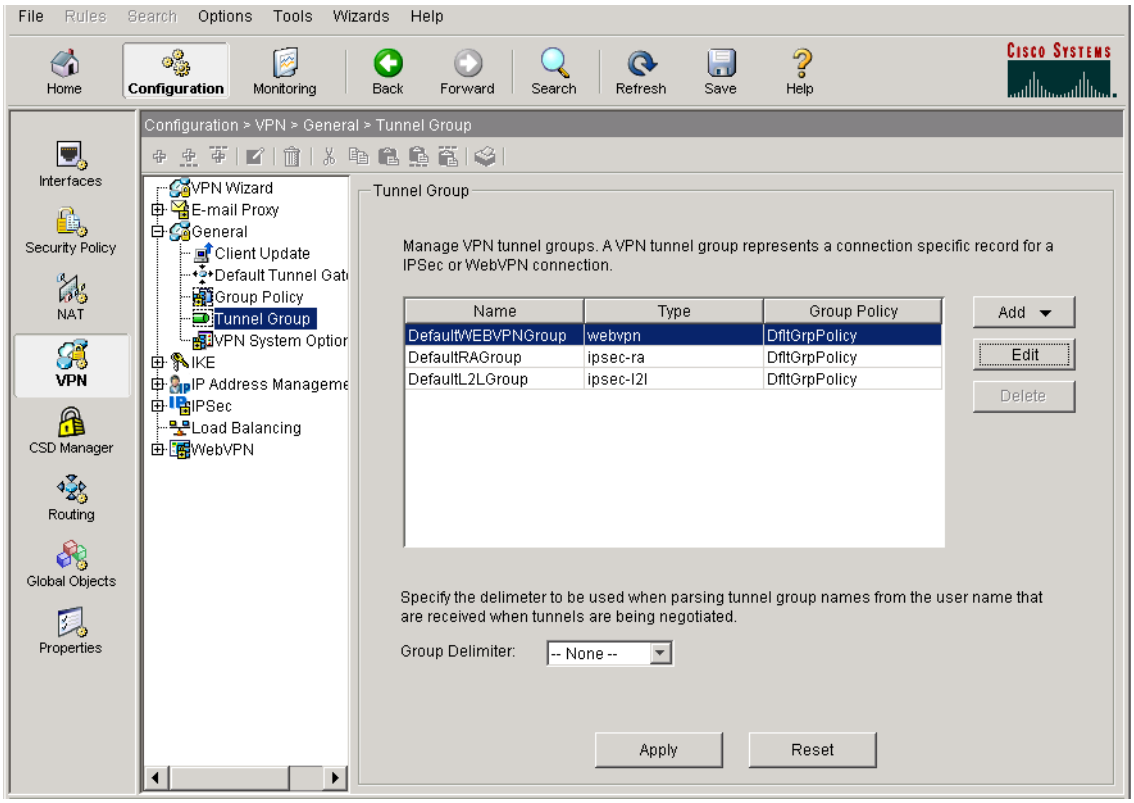
Figure 3-8 Add IP Pool Dialog



Enter the name of the new IP address pool. Enter the starting and ending IP addresses, and enter the subnet mask and click **OK**.

Step 3 Assign the IP address pool to a tunnel group. To do this, choose **Configuration >VPN > General > Tunnel Group**. The Tunnel Group panel appears (Figure 3-9):

Figure 3-9 Tunnel Group Window



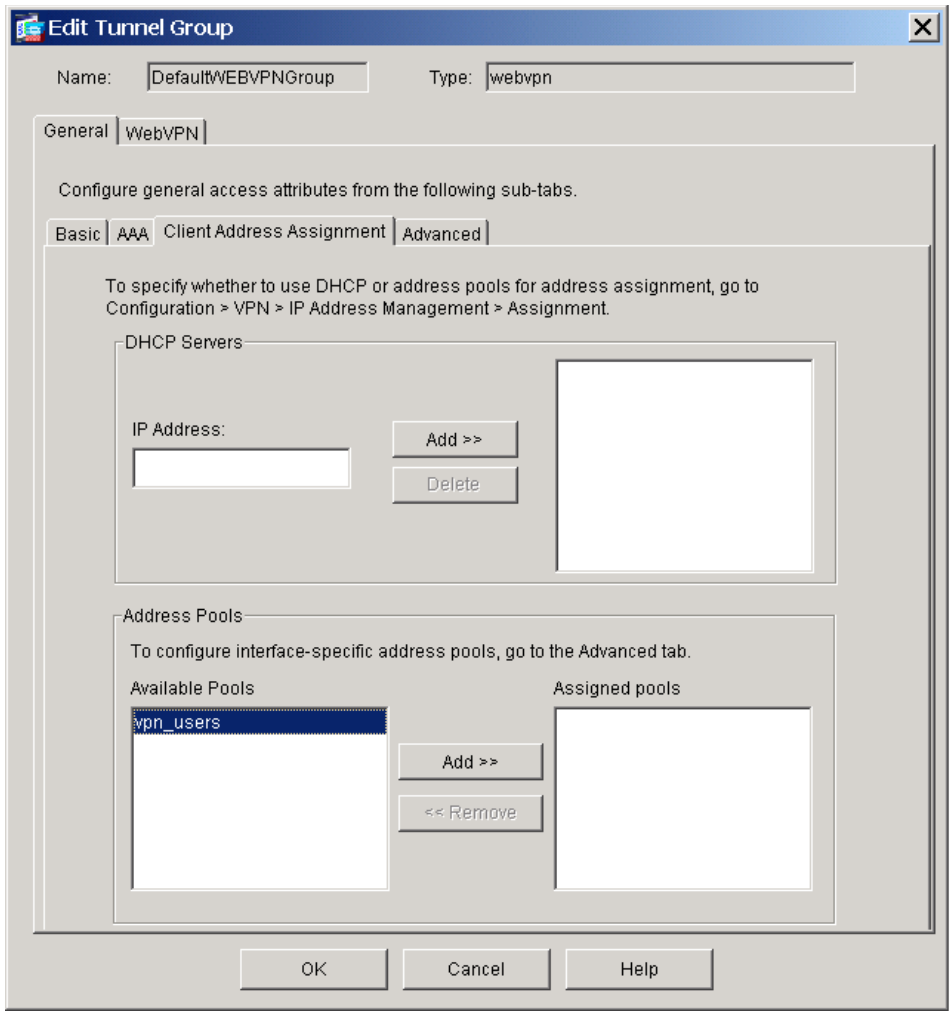
Step 4 Highlight a tunnel group in the table, and click **Edit.**

The Edit Tunnel Group dialog appears.

Step 5 Click the **Client Address Assignment** tab.

The **Client Address Assignment** tab appears (Figure 3-10), containing the Address Pools group box:

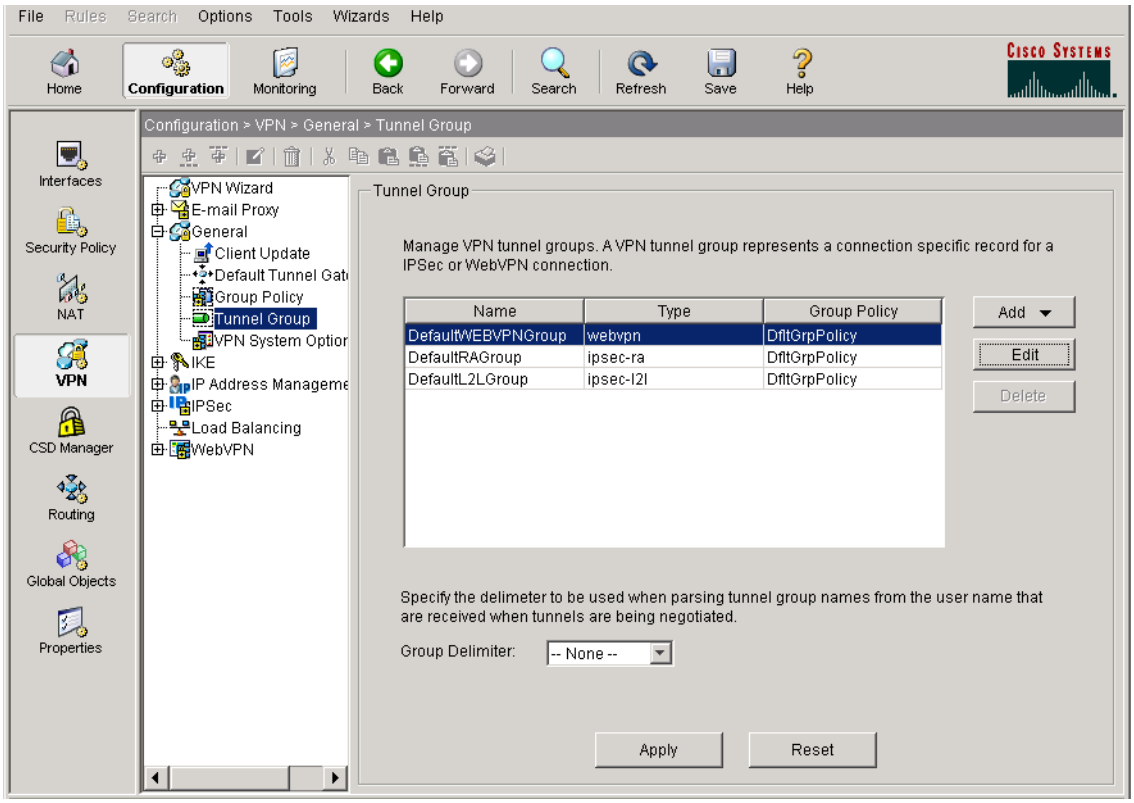
Figure 3-10 Edit Tunnel Group, General Tab, Client Address Assignment Tab



In the Address Pools group box, choose an address pool to assign to the tunnel group and click **Add**.

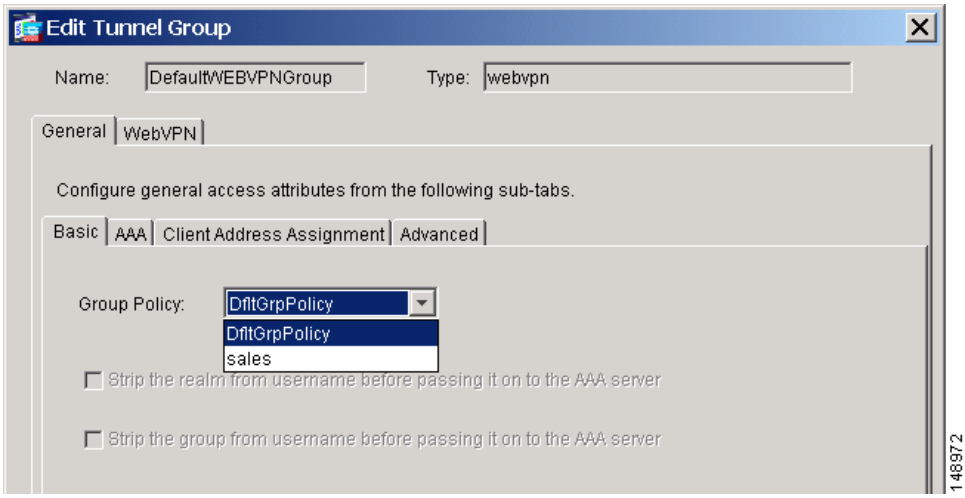
Step 6 Assign a default group policy to the tunnel group. Select **Configuration > VPN > General > Tunnel Group**. The Tunnel Group window appears (Figure 3-11).

Figure 3-11 Tunnel Group Window



Choose a WebVPN tunnel group from the table, and click **Edit**. The Edit Tunnel Group dialog, **General** tab appears (Figure 3-12).

Figure 3-12 Edit Tunnel Group Dialog, General Tab, Basic Tab

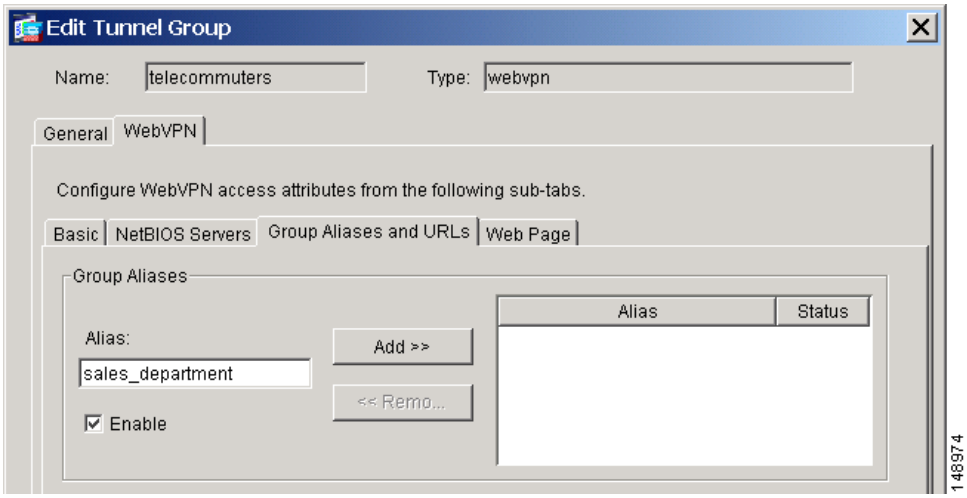


Choose a group policy in the Group Policy list and click **OK**.

Step 7 Create and enable a group alias that appears in the group list on the WebVPN Login page.

Click the **WebVPN** tab, and then click the **Group Aliases and URLs** tab. The Group Aliases and URLs tab appears (Figure 3-13):

Figure 3-13 Edit Tunnel Group Dialog, WebVPN Tab, Group Aliases and URLs Tab



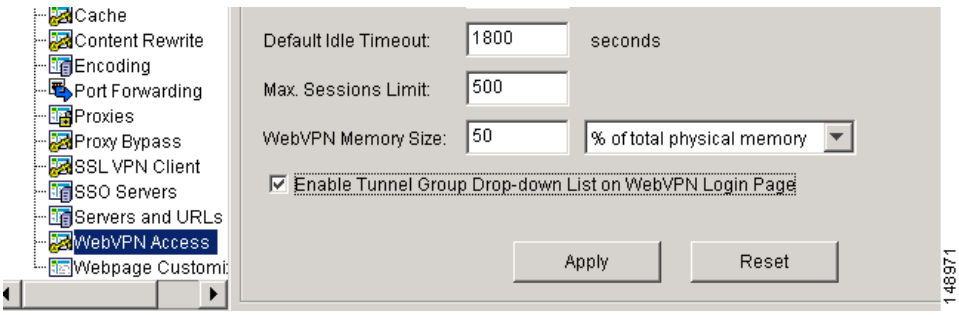
Enter the name of the new alias in the Alias field. Click **Add** to add it as a new alias.

Click the **Enable** check box to enable group aliases and URLs.

Step 8 Enable the display of the tunnel-group list on the WebVPN Login page.

Choose **Configuration > VPN > WebVPN > WebVPN Access**. The WebVPN Access panel appears (Figure 3-14). Click the **Enable Tunnel Group Drop-Down List on WebVPN Login Page** check box, and click **Apply**.

Figure 3-14 WebVPN Access Window, Enable Tunnel Group Drop-Down List on WebVPN Login Page Check Box

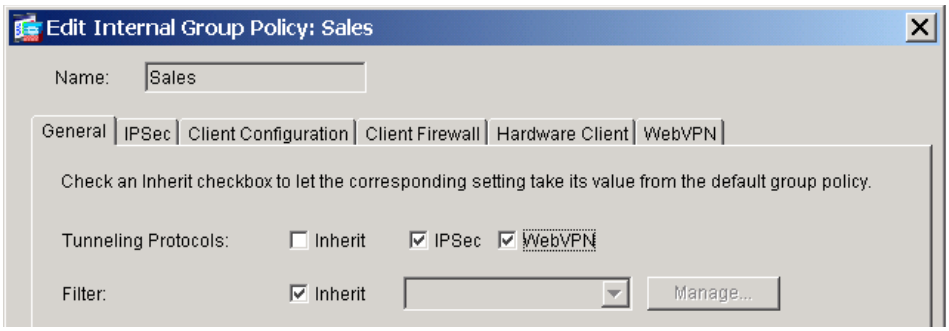


Step 9 Identify WebVPN as a permitted VPN tunneling protocol for the group or user.

Choose **Configuration > VPN > General > Group Policy** from the navigation pane. Highlight the group policy in the Group Policy table, and click **Edit**.

The General Tab of the Edit Internal Group Policy dialog appears (Figure 3-15):

Figure 3-15 Edit Internal Group Policy, GeneralTab



Check the **WebVPN** check box to include WebVPN as a tunneling protocol.

Step 10 Configure SVC features for a user or group. There features are shown in the **SSL VPN Client** tab of both the Edit User Accounts dialog and the Edit Group Policy dialog.

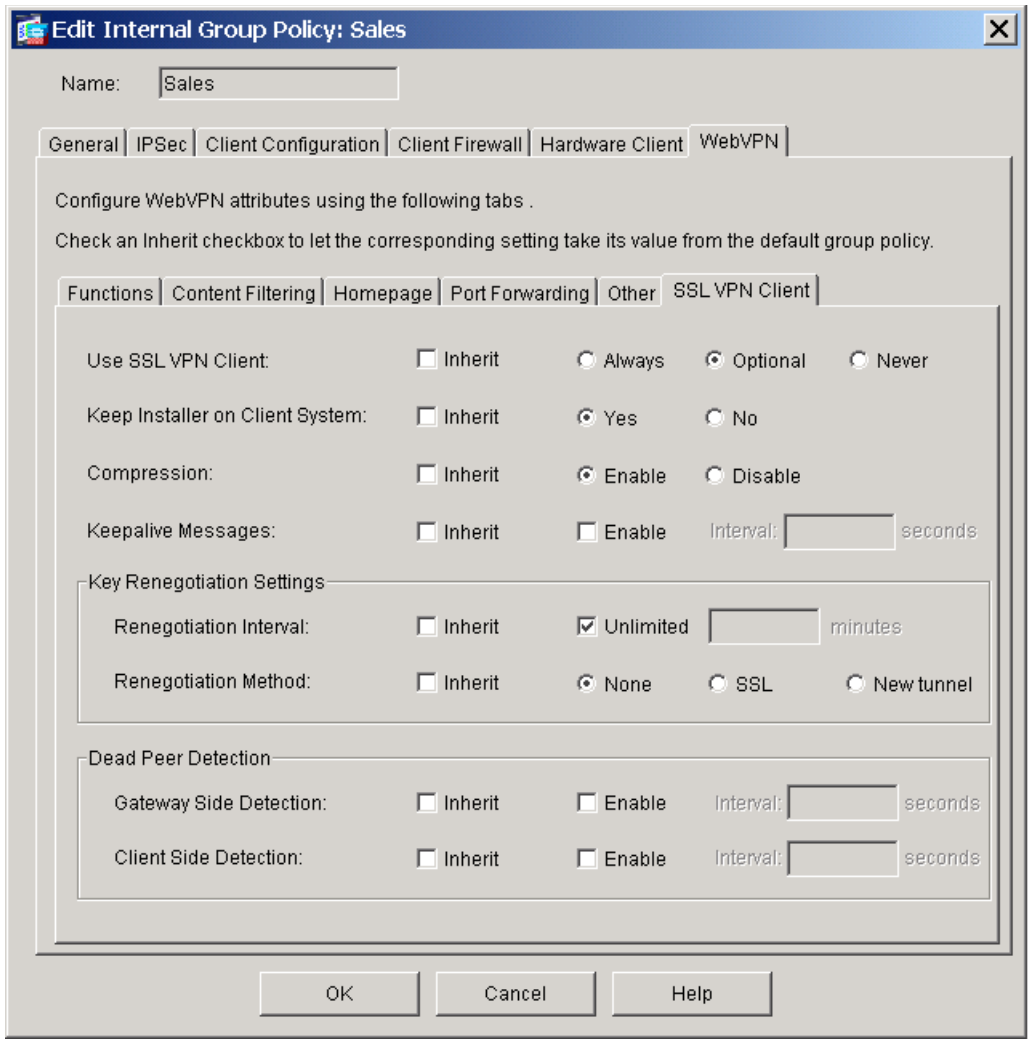
To display the **SSL VPN Client** tab For users:

- Click **Configuration > Properties > Device Administration > User Accounts**. The User Accounts panel appears.
- Choose a user in the table, and click **Edit**. The Edit User Account dialog, **General** tab appears.
- Click the **WebVPN** tab, and then click the **SSL VPN** tab. The **SSL VPN Client** tab appears Figure 3-16.

To display the **SSL VPN Client** tab for groups, do the following:

- Click **Configuration > VPN > WebVPN > Group Policies**. The Group Policy panel appears.
- Choose a group policy in the table, and click **Edit**. The Edit Internal Group Policy dialog, **General** tab appears.
- Click the **WebVPN** tab, and then click the **SSL VPN** tab. The **SSL VPN Client** tab appears. It is identical to the **SSL VPN Client** tab displayed for user accounts in Figure 3-16, but it does not include **Inherit** check boxes for the features.

Figure 3-16 SSL VPN Client Tab



Note For user accounts, the **SSL VPN Client** tab includes the additional **Inherit** check box for every SVC feature. If you check the **Inherit** check box, the feature is configured according to the setting in the group policy of the user.

Configure the following features on the SSL VPN Client tab:

Use SSL VPN Client—Require the SVC, make it optional, or disable it for the user or group.

Keep Installer on Client System—Enable to allow permanent SVC installation on the remote computer. Enabling prevents the automatic uninstalling feature of the SVC. The SVC remains installed on the remote computer for subsequent SVC connections, reducing the SVC connection time for the remote user.

Compression—SVC compression increases the communications performance between the security appliance and the SVC by reducing the size of the packets being transferred.

Keepalive Messages—Check the **Enable** checkbox to enable and adjust the interval of keepalive messages to ensure that an SVC connection through a proxy, firewall, or NAT device remains open, even if the device limits the time that the connection can be idle.

Adjusting the interval also ensures that the SVC does not disconnect and reconnect when the remote user is not actively running a socket-based application, such as Microsoft Outlook or Microsoft Internet Explorer.

The Seconds field specifies the interval of the messages in the range of 15 to 600 seconds.

Rekey Negotiation Settings—When the security appliance and the SVC perform a rekey, they renegotiate the crypto keys and initialization vectors, increasing the security of the connection.

- **Renegotiation Interval—**Clear the **Unlimited** check box to specify the number of minutes from the start of the session until the rekey takes place, from 1 to 10080 (1 week).
- **Renegotiation Method—**Check the **None** check box to disable rekey, check the **SSL** check box to specify SSL renegotiation during a rekey, or check the **tunnel** check box to establish a new tunnel during SVC rekey.

Dead Peer Detection—Dead Peer Detection (DPD) ensures that the security appliance (gateway) or the SVC can quickly detect a condition where the peer is not responding, and the connection has failed.

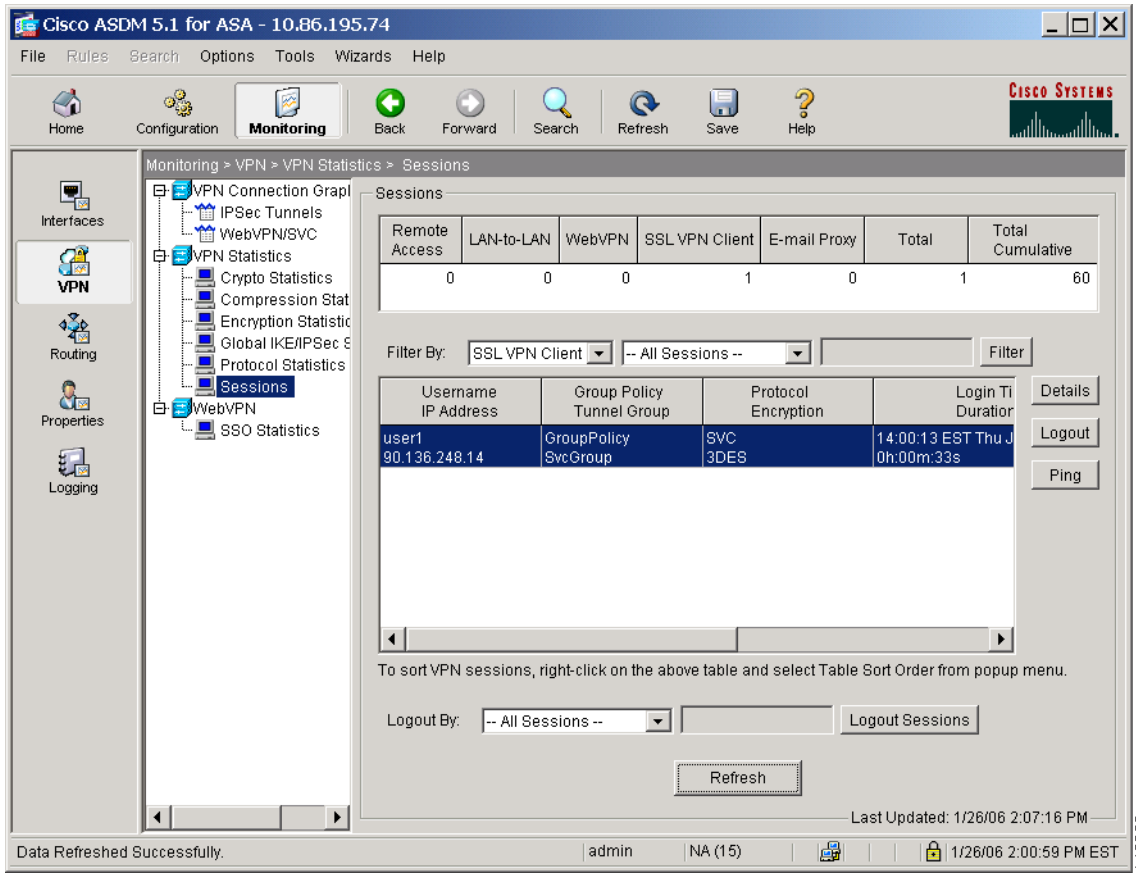
- **Gateway Side Detection—**Check the **Enable** check box to specify that DPD is performed by the security appliance (gateway). Enter the interval, from 30 to 3600 seconds, with which the security appliance performs DPD.
- **Client Side Detection—**Check the **Enable** check box to specify that DPD is performed by the SVC (client). Enter the interval, from 30 to 3600 seconds, with which the SVC performs DPD.

Viewing SVC Sessions

You can view information about active SVC sessions in the Sessions window.

Choose **Monitoring > VPN > VPN Statistics > Sessions**. The Sessions window appears (Figure 3-17)

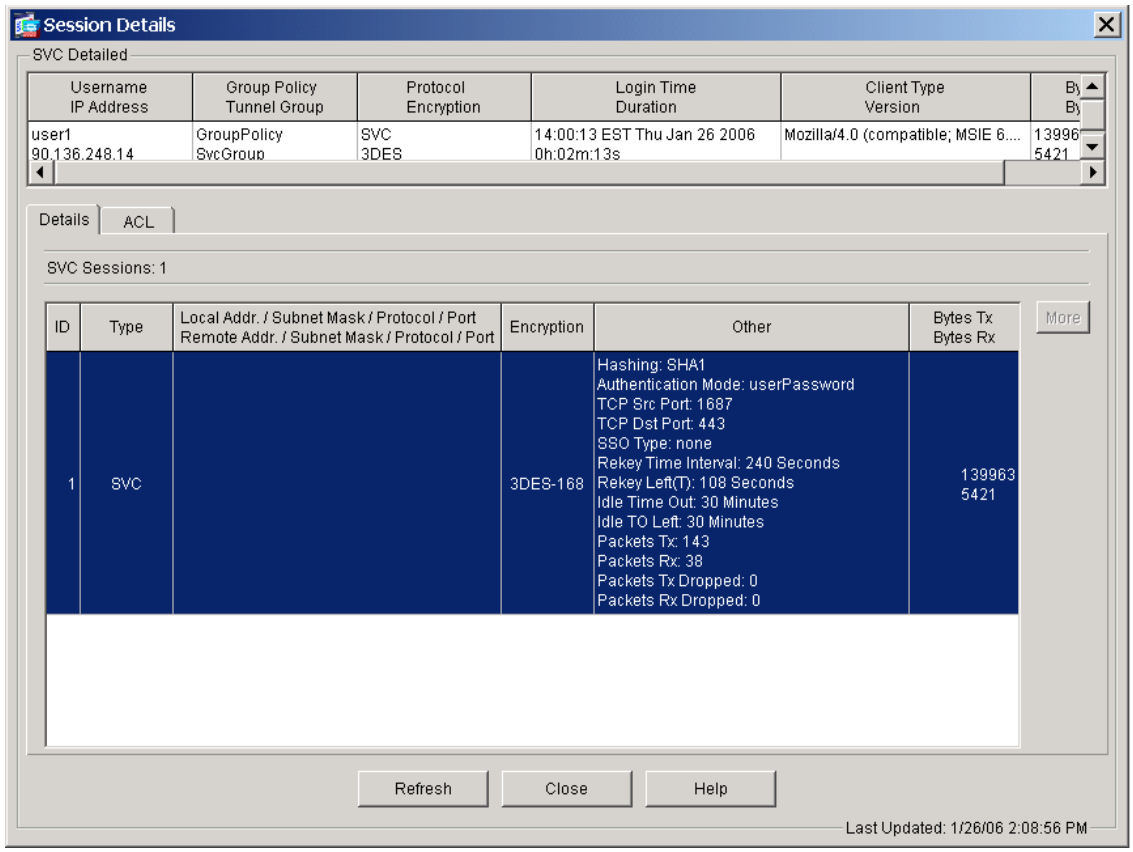
Figure 3-17 VPN Statistics Sessions Window



You can view details about active SVC sessions in the Session Details window.

Choose a session in the session table, and click **Details**. The Session Details window appears (Figure 3-18):

Figure 3-18 Session Details Window

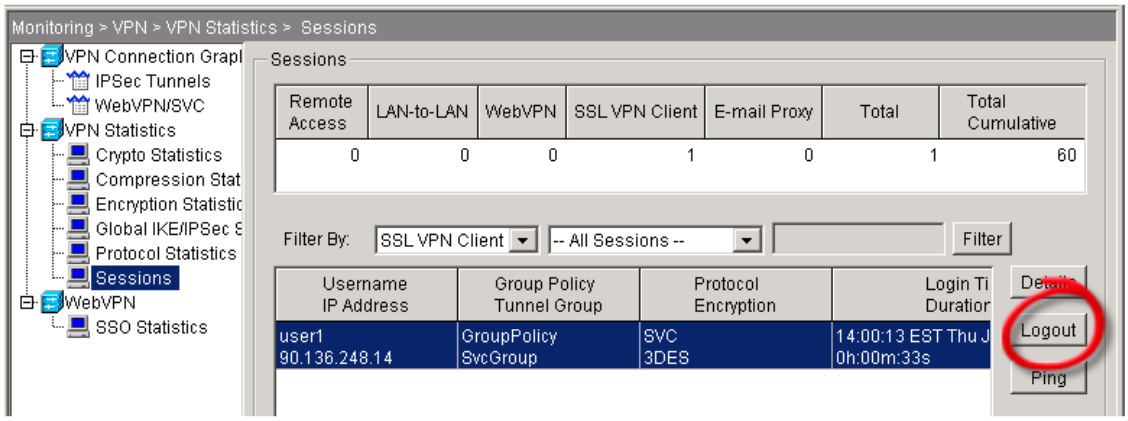


Logging Off SVC Sessions

To log off all SVC sessions, choose the session that you want to terminate from the list of active sessions in the Session table.

Click **Logout**. The session terminates.

Figure 3-19 Logging Off Sessions



Configuring Client Update for Windows and VPN 3002 Clients

ASDM encompasses two kinds of client update: one that supports Windows clients and VPN 3002 hardware clients through a tunnel group, and the other that supports ASA devices acting as an auto-update server. This chapter describes how to configure the tunnel-group client-update function for Windows clients and VPN 3002 hardware clients.

The client update feature lets administrators at a central location automatically notify VPN client users that it is time to update the VPN client software and the VPN 3002 hardware client image. If the client is already running a software version on the list of revision numbers, it does not need to update its software. If the client is not running a software version on the list, it should update. This procedure applies only to the IPSec remote-access tunnel-group type.

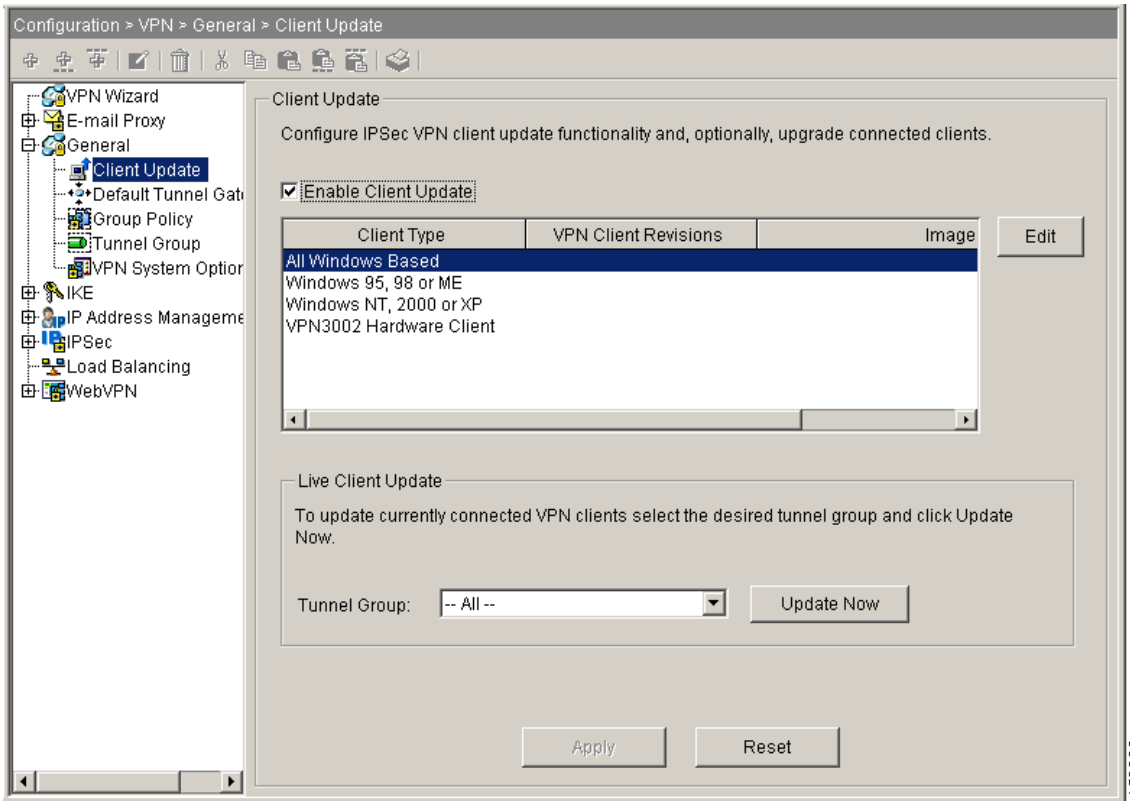
Remote users might be using outdated VPN software or hardware client versions. You can perform a client-update at any time to do the following functions:

- Enable updating client revisions
- Specify the types and revision numbers of clients to which the update applies
- Provide a URL or IP address from which to get the update
- Optionally notify Windows client users that they should update their VPN client version.
- For Windows clients, you can provide a mechanism for users to accomplish the update.
- For VPN 3002 hardware client users, the update occurs automatically, with no notification.

To configure a client-update, perform the following steps.

Step 1 Go to the client update window by choosing the path **Configuration > VPN > General > Client Update**. The Client Update window opens (Figure 4-1).

Figure 4-1 Client Update Window



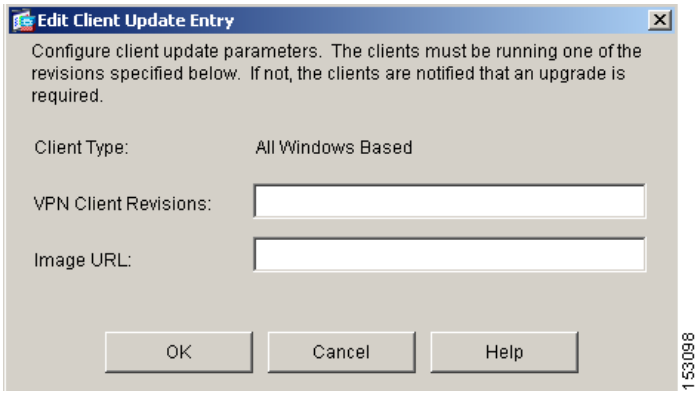
Step 2 Enable client update by checking the Enable Client Update check box.

Step 3 Select the type of client for which you want to apply the client update. The available client types are All Windows-Based, Windows 95, 98 or ME, Windows NT 4.0, 2000 or XP, and VPN 3002 Hardware Client.

If the client is already running a software version on the list of revision numbers, it does not need to update its software. If the client is not running a software version on the list, it should update. You can specify up to three of these client update entries. The All Windows Based selection covers all of the allowable Windows platforms. If you select this, do not specify the individual Windows client types.

Step 4 To specify the acceptable client revisions and the source for the updated software or firmware image for the client update, click Edit. The Edit Client Update Entry window (Figure 4-2) appears, showing the client type selection.

Figure 4-2 Edit Client Update Entry Window



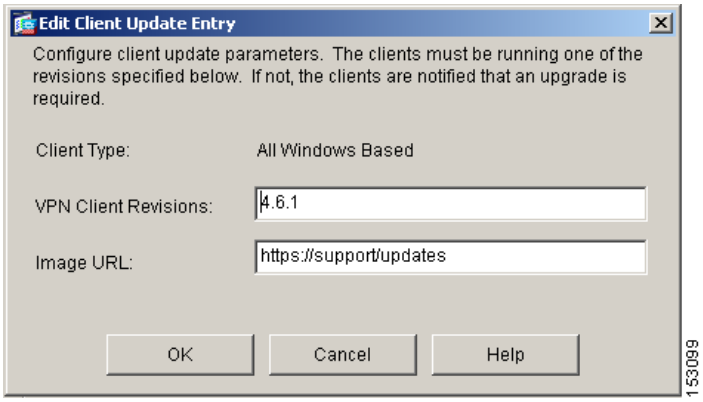
Step 5 Specify the client update that you want to apply to all clients of the selected type across the entire security appliance. That is, specify the type of client, the URL or IP address from which to get the updated image, and the acceptable revision number or numbers for that client. You can specify up to four revision numbers, separated by commas. Your entries appear in the appropriate columns the table on the Client Upgrade window after you click OK.

If the user's client revision number matches one of the specified revision numbers, there is no need to update the client.

Note For all Windows clients, you must use the protocol http:// or https:// as the prefix for the URL. For the VPN 3002 hardware client, you must specify protocol tftp:// instead.

Figure 4-3 shows an example that initiates a client update for all Windows clients for a remote-access tunnel-group running revisions older than 4.6.1 and specifies the URL for retrieving the update as https://support/updates:

Figure 4-3 Edit Client Update Entry Example



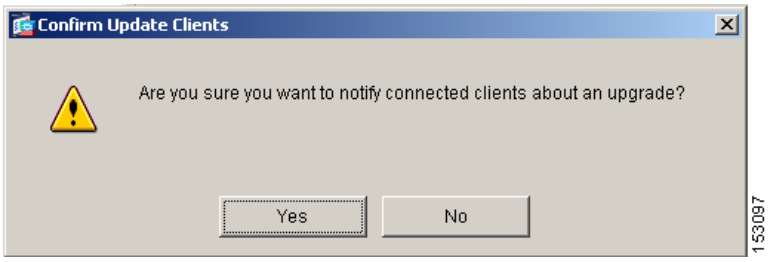
Alternatively, you can configure client update just for individual client types, rather than for all Windows clients. (See Step 3.)

VPN 3002 clients update without user intervention and users receive no notification message.

You can have the browser automatically start an application by including the application name at the end of the URL; for example: **`https://support/updates/vpnclient.exe`**.

Step 6 Optionally, you can send a notice to active users with outdated Windows clients that their client needs updating. To send this notice, use the Live Client Update area of the Client Update window. Select the tunnel group (or All) and click Update Now. A dialog box appears (Figure 4-4), asking you to confirm that you want to notify connected clients about the upgrade.

Figure 4-4 Confirm Update Clients Dialog Box



The designated users see a pop-up window, offering them the opportunity to launch a browser and download the updated software from the site that you specified in the URL. The only part of this message that you can configure is the URL. (See Step 2 or 3.) Users who are not active get a notification message the next time they log on. You can send this notice to all active clients on all tunnel groups, or you can send it to clients on a particular tunnel group.

If the user's client revision number matches one of the specified revision numbers, there is no need to update the client, and no notification message is sent to the user. VPN 3002 clients update without user intervention and users receive no notification message.

Configuring DDNS Updates

This chapter describes how to configure Dynamic DNS updates, a process by which two types of DNS resource records (RRs) are updated with the latest IP address and hostname information. There are several scenarios for updating these records; this chapter presents the procedure for configuring the following common scenario:

The DHCP client asks the DHCP server to update both DNS RRs. The server, configured to update PTR RRs only, honors the client request and updates both the A and PTR RRs.

This chapter includes the following sections:

Overview of DDNS Resource Records

DDNS provides address and domain name mappings so hosts can find each other even though their DHCP-assigned IP addresses change frequently. Mappings are contained in two types of records that reside on the DNS server. These records, *A* RRs and *PTR* RRs, allow identification of a host either by IP address or by domain name. A RRs contain domain name to IP address mappings while PTR RRs contain IP address to domain name mappings. Of the two methods for performing DDNS updates to these records—the IETF standard defined by RFC 2136 and a generic HTTP method—the security appliance supports the IETF method in this release.

Each of the records can be updated by either the DHCP server or the client depending upon how you configure the updates. The client can request that the server perform the updates on its behalf. However, you must configure the server to either honor the client request or override it.

To update the PTR RR, the DHCP server must know the Fully Qualified Domain Name of the client. The client provides an FQDN to the server using a DHCP option called Client FQDN.

This chapter presents the steps for configuring the DHCP server to update both the A RR and the PTR RR. This is one of the most common configurations. Other configuration scenarios discussed in the *Cisco Security Appliance Command Line Configuration Guide* include:

- The DHCP client updates both the A and PTR RRs for static IP addresses.
- The DHCP client updates both the A and PTR RRs. The DHCP server honors the client update request. FQDN provided through configuration.

- The DHCP client includes the FQDN option instructing the server not to update either RR. The server overrides client request and updates both RRs.
- The DHCP client updates the A resource record while the DHCP server updates the PTR records. The client uses the domain name from the server to form the fully qualified domain name.

Overview of DDNS Example: Server Updates Both Records

This section configures the DHCP server to perform only PTR RR updates by default. However, the server honors the client request that it perform both A and PTR updates.

.To complete this configuration example, perform the following tasks.

1. Define the DDNS update method.
2. Assign the DDNS update method to a security appliance interface.
3. Configure the DHCP server.

Note Prerequisite steps that are outside the scope of this procedure include configuring DHCP servers, configuring DNS clients, and enabling DHCP on interfaces.

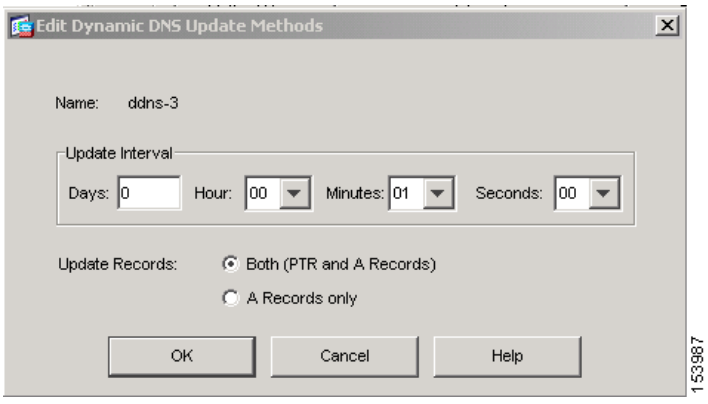
Defining an Update Method

To define a DDNS update method, perform the following steps:

Step 1 In the **Configuration > Properties > DNS > Dynamic DNS** window, click **Add**.

The Edit Dynamic DNS Update Methods dialog box appears as shown in Figure 5-1.

Figure 5-1 Edit Dynamic DNS Update Methods Dialog Box



Step 2 In the Name field, enter a DDNS method name.

In this example, we name the method DDNS-3.

Step 3 In the Days field, enter the number of days between update attempts.

Days can be from 0 to 364.

Step 4 From the Hours menu, choose a number of hours between update attempts.

Step 5 From the Minutes menu, choose a number of minutes between update attempts.

In this example, we schedule an update attempt every minute.

Step 6 From the Seconds menu, choose a number of seconds between update attempts.

Note These time units are additive. That is, if you enter 0 days, 0 hours, 5 minutes and 15 seconds, the update method will attempt an update every 5 minutes and 15 seconds for as long as the method is active

Step 7 Next to Update Records, click either the **Both (PTR and A Records)** radio button or the **A Records only** radio button to configure the DHCP client to update records.

Note You can select either radio button because the interface or the DHCP server can be configured to override the method setting.

Step 8 Click **OK** to accept the update method configuration.

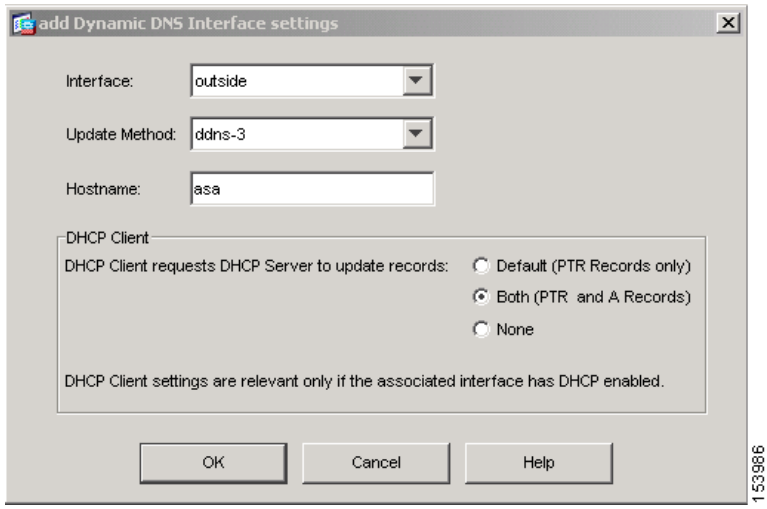
Assigning the Update Method to an Interface

To assign a DDNS update method to a security appliance interface, perform the following steps:

Step 1 In the **Configuration > Properties > DNS > Dynamic DNS** window, click **Add**.

The Add Dynamic DNS Interface Settings dialog box appears as shown in Figure 5-2.

Figure 5-2 Add Dynamic DNS Interface Settings Dialog Box



Step 2 Select the interface to be configured from the Interface menu.

In this example, we select the outside interface.

Step 3 Select the update method to be applied to the interface from the Update Method menu.

In this example, we select DDNS-3.

Step 4 Enter the Dynamic DNS hostname in the Hostname field.

In this example, we enter asa.

Step 5 In the DHCP Client area, click **Both (PTR and A Records)**.

Step 6 Click **OK** to accept the interface configuration settings.

The Add Dynamic DNS Interface Settings dialog box closes.

Step 7 At the bottom of the Dynamic DNS panel, click Both (PTR Records and A Records) to set the global DHCP server update setting to update both resource records.

Step 8 Click Apply to add the new DDNS settings to the running security appliance configuration.

Configuring the DHCP Server

To configure the DHCP server to update PTR records and to also honor DHCP client update requests, perform the following steps:

Step 1 In the **Configuration > Properties > DHCP Services > DHCP Server** window, select the DHCP server you want to update the DNS records.

Step 2 In the Dynamic DNS Settings for DHCP Server area, perform the following steps:

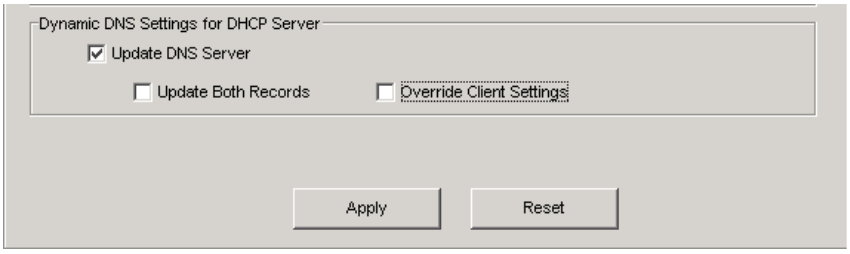
a. Check the **Update DNS Clients** check box.

b. Uncheck the **Update Both Records** check box.

c. Uncheck the **Override Client Settings** check box.

The Dynamic DNS Settings for DHCP Server area should appear as shown in Figure 5-3.

Figure 5-3 The Dynamic DNS Settings for DHCP Server area.



Step 3 Click **Apply** to add the DHCP server setting to the security appliance running configuration.

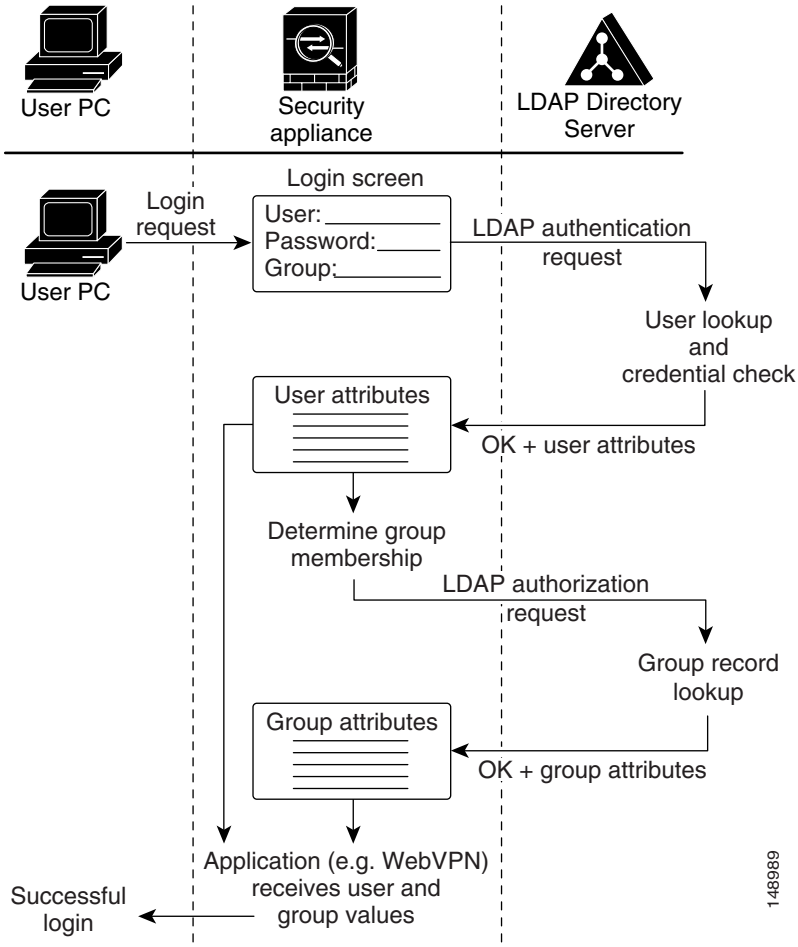
Configuring an LDAP AAA Server

This chapter presents an example configuration procedure for configuring security appliance user authentication and authorization using a Microsoft Active Directory Server (LDAP) that is on the same internal network as the security appliance. It includes the following sections.

Overview of LDAP Transactions

Figure 6-1 shows the major transactions in security appliance user authentication and authorization using an LDAP directory server.

Figure 6-1 LDAP Authentication and Authorization Transaction Flow



Creating an LDAP Attribute Map

To configure the security appliance for LDAP authentication and authorization, you must first create an LDAP attribute map which maps customer-defined attribute names to Cisco LDAP attribute names. This prevents you from having to rename your existing attributes using the Cisco names that the security appliance understands.

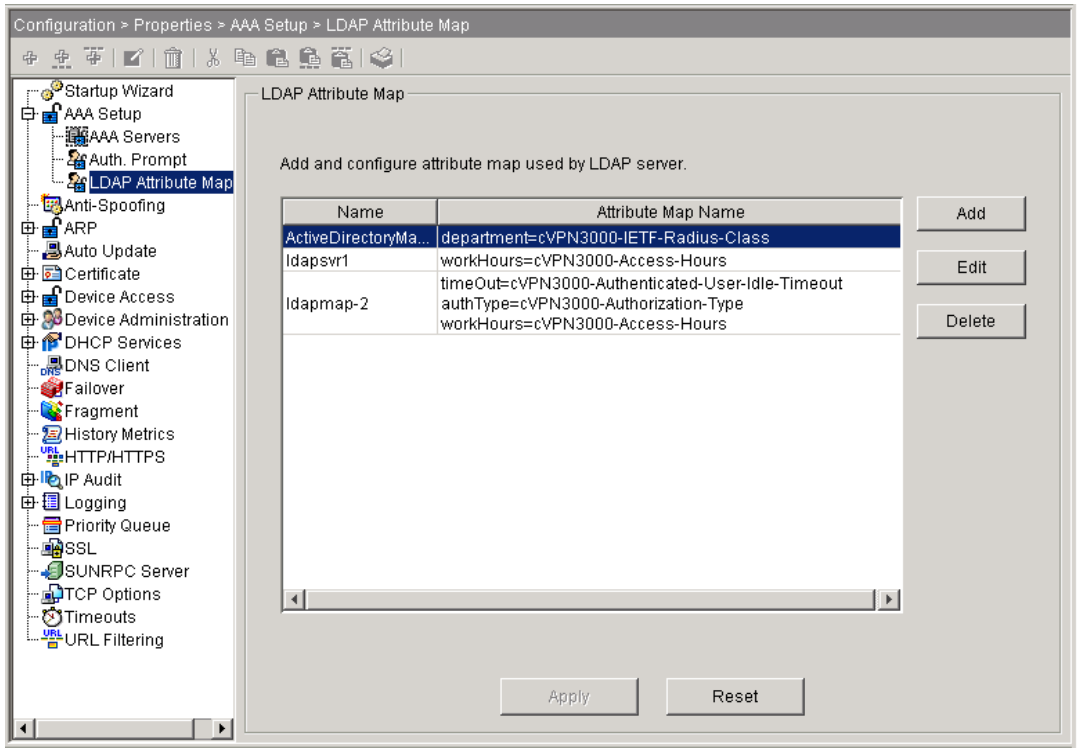
Note To use the attribute mapping features correctly, you need to understand the Cisco LDAP attribute names and values as well as the user-defined attribute names and values. See the *Cisco Security Appliance Command Line Configuration Guide* appendix, "Configuring an External Server for Authorization and Authentication" for the list of Cisco LDAP attributes.

To create a new LDAP attribute map, perform the following steps:

Step 1 In the Cisco ASDM window, choose **Configuration > Properties > AAA Setup > LDAP Attribute Map**.

The LDAP Attribute Map area appears in the window on the right as shown in Figure 6-2.

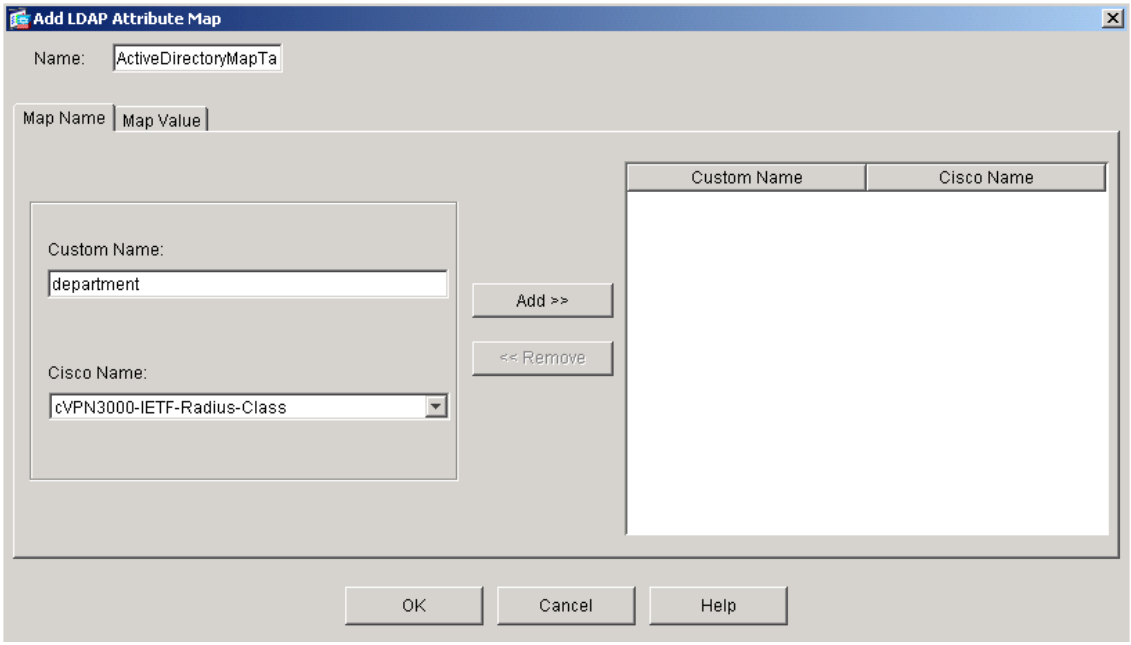
Figure 6-2 LDAP Attribute Map Area



Step 2 In the LDAP Attribute Map area, click **Add**.

The Add LDAP Attribute Map dialog box appears as shown in Figure 6-3.

Figure 6-3 Add LDAP Attribute Map Dialog Box - Map Name Tab Selected



Step 3 In the Name field above the tabs, enter a name for the LDAP attribute map.

In this example, we name the attribute map ActiveDirectoryMapTable.

Step 4 If the Map Name tab is not selected, choose it now.

Step 5 In the Custom Name (user-defined attribute name) field on the Map Name tab, enter the name of an attribute that you want to map to a Cisco attribute name.

In this example, the custom name is *department*.

Step 6 Choose a Cisco name from the Cisco Name menu. The custom name maps to this Cisco name.

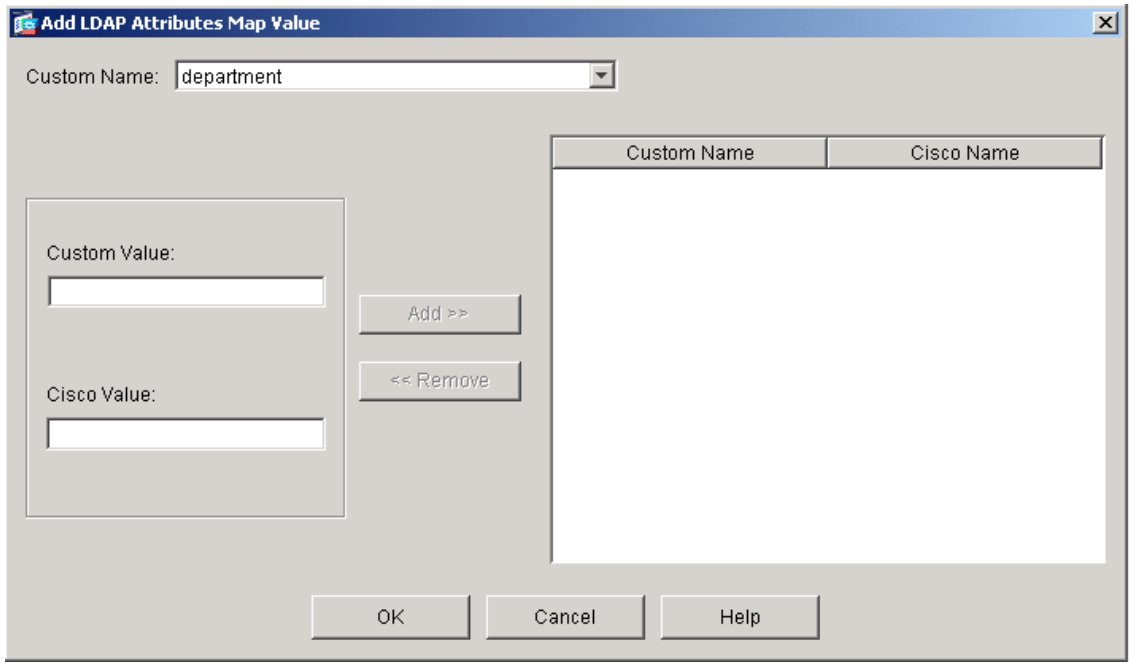
In this example, the Cisco name is cVPN3000-IETF-Radius-Class. As shown in Figure 6-1, the security appliance receives the user attributes from the authentication server upon validation of the user credentials. If a class attribute is among the user attributes returned, the security appliance interprets it as the group policy for that user, and it sends a request to the AAA server group configured for this group policy to obtain the group attributes.

Step 7 Click **Add** to include the name mapping in the attribute map.

Step 8 Click the **Map Value** tab and then click **Add** on the Map Value tab.

The Add LDAP Attributes Map Value dialog box appears as shown in Figure 6-4.

Figure 6-4 Add LDAP Attributes Map Value Dialog Box



Step 9 From the Custom Name menu, choose the custom attribute for which you want to map a value.

Step 10 Enter the custom (user-defined) value in the Custom Value field.

Step 11 Enter the Cisco value in the Cisco Value field.

Step 12 Click **Add** to include the value mapping in the attribute map.

Step 13 Repeat Step 4 through Step 12 for each attribute name and value to be mapped.

Step 14 After you have completed mapping all the names and values, click **OK** at the bottom of the Add LDAP Attribute Map window.

Step 15 Click **Apply** to complete the new LDAP attribute map and add it to the running security appliance configuration.

Configuring AAA Server Groups and Servers

Next, you configure AAA server groups and the AAA servers that go into them. You must configure two AAA server groups. You configure one server group as an authentication server group containing an authentication server that requests an LDAP search of the user records. You configure the other server group as an authorization server group containing an authorization server that requests an LDAP search of the group records. One notable difference between the two groups is that the AAA servers have different base DN fields to specify different Active Directory folders to search.

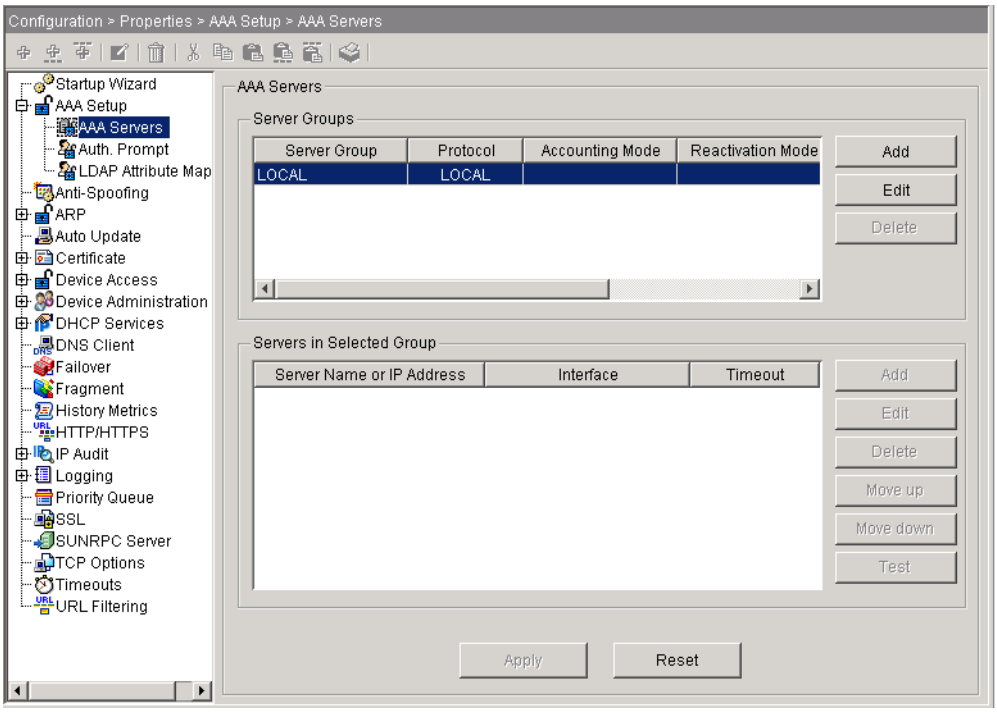
Creating the LDAP AAA Server Groups

To configure the two server groups, perform the following steps:

Step 1 In the Cisco ASDM window, choose **Configuration > Properties > AAA Setup > AAA Servers**.

The AAA Servers area appears in the right half of the window as shown in Figure 6-5.

Figure 6-5 The ASDM Window with AAA Servers Selected

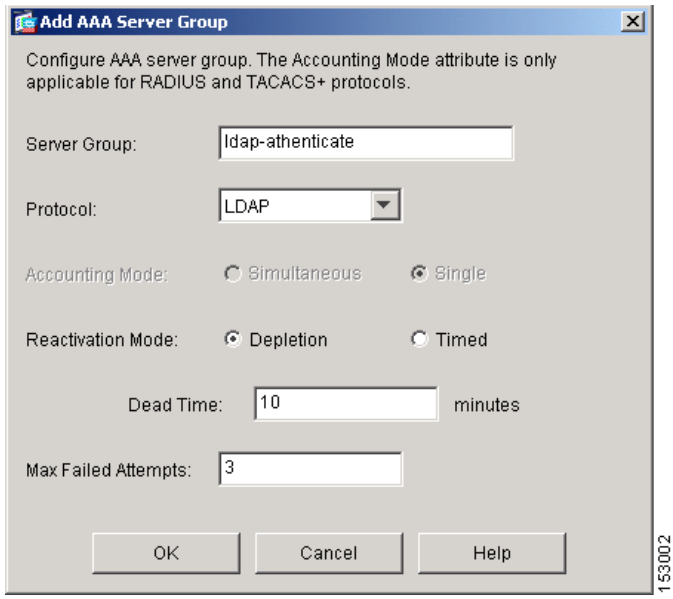


The fields in the AAA Servers area are grouped into two areas: the Server Groups area and the Servers In The Selected Group area. The Server Groups area lets you configure AAA server groups and the protocols the security appliance uses to communicate with the servers listed in each group.

Step 2 In the Server Groups area, click **Add**.

The Add AAA Server Group dialog box appears as shown in Figure 6-6.

Figure 6-6 The Add AAA Server Group Dialog Box



Step 3 Enter the name of the server group in the Server Group field.

Use different names for the authentication server group and the authorization server group. In this example, we name the authentication server group *ldap-authenticat* (authenticate is truncated because of a sixteen character maximum) and the authorization server group *ldap-authorize*.

Step 4 Choose **LDAP** from the Protocol menu.

Step 5 For the Reactivation Mode, choose one of the following:

- **Depletion**—Configures the security appliance to reactivate failed servers only after all of the servers in the group are inactive.
- **Timed**—Configures the security appliance to reactive failed servers after 30 seconds of down time.

Step 6 In the Dead Time field, enter the number of minutes that elapse between the disabling of the last server in the group and the subsequent reenabling of all servers.

This field is not available if you selected Timed mode in Step 5.

Step 7 In the Max Failed Attempts field, enter the number of failed connection attempts (1 through 5) allowed before declaring a nonresponsive server inactive.

Step 8 Click **OK** to enter the newly configured server into the Server Groups table.

Step 9 Repeat Step 2 through Step 8 for the second AAA server group. When done, you should have an authentication server group and an authorization server group.

Configuring the LDAP AAA Servers

For each of the two AAA server groups, you next configure a AAA server. Again, one server is for authentication and one for authorization.

To add a new LDAP AAA server to each of the AAA server groups, perform the following steps:

Step 1 In the Cisco ASDM window, choose **Configuration > Properties > AAA Setup > AAA Servers**.

The AAA Servers area appears in the right half of the window.

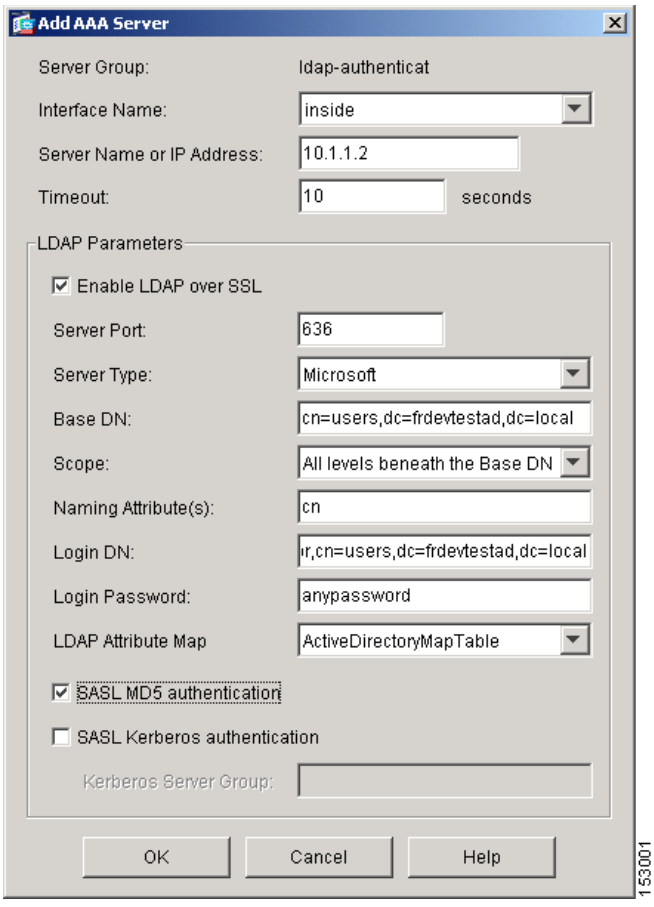
Step 2 In the Server Group table, click the LDAP server group to which you want to add the LDAP server.

In this example, we configure the authentication server in the ldap-authenticat group and the authorization server in the ldap-authorize group.

Step 3 In the Servers in Selected Group area, click **Add**.

The Add AAA Server dialog box appears as shown in Figure 6-7.

Figure 6-7 The Add AAA Server Dialog Box



Step 4 From the Interface Name menu, choose either:

- **Inside** if your LDAP server is on your internal network

  -or-

- **Outside** if your LDAP server is on an external network

In our example, the LDAP server is on the internal network.

Step 5 Enter the server name or IP address in the Server Name or IP Address field.

In our example, we use the IP address.

Step 6 In the Timeout field, enter the timeout interval in seconds.

This is the time after which the security appliance gives up on the request to the primary AAA server. If there is a standby server in the server group, the security appliance sends the request to the backup server.

Step 7 In the LDAP Parameters area, check **Enable LDAP over SSL** if you want all communications between the security appliance and the LDAP directory to be encrypted with SSL.

Warning **If you do not check Enable LDAP over SSL, the security appliance and the LDAP directory exchange all data in the clear, including sensitive authentication and authorization data.**

Step 8 Enter the server port to use in the Server Port field.

This is the TCP port number by which you access the server.

Step 9 From the Server Type menu, choose one of the following:

- **Sun Microsystems JAVA System Directory Server** (formerly the Sun ONE Directory Server)

  - or -

- **Microsoft Active Directory**

  - or -

- **Detect automatically**

The security appliance supports authentication and password management features only on the Sun Microsystems JAVA System Directory Server (formerly named the Sun ONE Directory Server) and the Microsoft Active Directory. By selecting Detect automatically, you let the security appliance determine if the server is a Microsoft or a Sun server.

Note The DN configured on the security appliance to access a Sun directory server must be able to access the default password policy on that server. We recommend using the directory administrator, or a user with directory administrator privileges, as the DN. Alternatively, you can place an ACI on the default password policy.

Step 10 Enter one of the following into the Base DN field:

- The base DN of the Active Directory folder holding the user attributes (typically a users folder) if you are configuring the authentication server

  - or -

- The base DN of the Active Directory folder holding the group attributes (typically a group folder) if you are configuring the authorization server

The base DN is the location in the LDAP hierarchy where the server should begin searching when it receives an authorization request. For example, OU=people, dc=cisco, dc=com.

Step 11 From the Scope menu, select one of the following:

- **One level beneath the Base DN**

  - or -

- **All levels beneath the Base DN**

The scope specifies the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request. One Level Beneath the Base DN specifies a search only one level beneath the Base DN. This option is quicker. All Levels Beneath the Base DN specifies a search of the entire subtree hierarchy. This option takes more time.

Step 12 In the Naming Attribute(s) field, enter the Relative Distinguished Name attribute that uniquely identifies an entry on the LDAP server.

Common naming attributes are Common Name (cn) and User ID (uid).

Step 13 In the Login DN field, perform one of the following:

- Enter the name of the directory object for security appliance authenticated binding. For example, cn=Administrator, cn=users, ou=people, dc=Example Corporation, dc=com.

  - or -

- Leave this field blank for anonymous access.

Some LDAP servers, including the Microsoft Active Directory server, require the security appliance to establish a handshake via authenticated binding before accepting requests for LDAP operations. The security appliance identifies itself for authenticated binding by including a Login DN field with the user authentication request. The Login DN field defines the security appliance authentication characteristics which should correspond to those of a user with administration privileges.

Step 14 Enter the password associated with the Login DN in the Login Password field.

The characters you type appear as asterisks.

Step 15 From the LDAP Attribute Map menu, choose the LDAP attribute map to apply to the LDAP server.

The LDAP attribute map translates user-defined LDAP attribute names and values into Cisco attribute names and values. To configure a new LDAP attribute map, see Creating an LDAP Attribute Map, page 6-2.

Step 16 Check **SASL MD5 Authentication** to use the MD5 mechanism of the Simple Authentication and Security Layer (SASL) to secure authentication communications between the security appliance and the LDAP server.

Step 17 Check **SASL Kerberos Authentication** to use the Kerberos mechanism of the Simple Authentication and Security Layer to secure authentication communications between the security appliance and the LDAP server.

Note If you configure more than one SASL method for a server, the security appliance uses the strongest method supported by both the server and the security appliance. For example, if both MD5 and Kerberos are supported by both the server and the security appliance, the security appliance selects Kerberos to secure communication with the server.

Step 18 If you checked SASL Kerberos authentication in Step 17, enter the Kerberos server group used for authentication in the Kerberos Server Group field.

Step 19 Repeat Step 3 through Step 18 to configure a AAA server in the other AAA server group.

Configuring the Group Policy for LDAP Authorization

After configuring the LDAP attribute map, the AAA server groups, and the LDAP servers within the groups, you next create an external group-policy that associates the group-name with the LDAP authorization server.

Note Comprehensive procedures for configuring group policies are provided elsewhere in this guide. The following steps are only those that apply to configuring AAA with LDAP.

To create a new group policy and assign the LDAP authorization server group to it, perform the following steps:

Step 1 In the Cisco ASDM window, select **Configuration > VPN > General > Group Policy.**

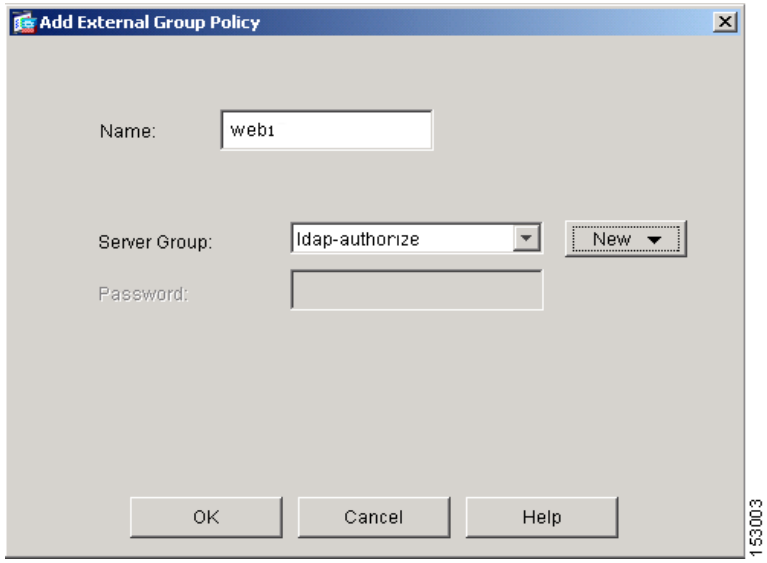
The Group Policy area appears in the right half of the window.

Step 2 Click **Add** and choose either **Internal Group Policy** or **External Group Policy**.

In this example, we choose External Group Policy because the LDAP server is external to the security appliance.

The Add Group Policy dialog box appears as shown in Figure 6-8.

Figure 6-8 Add Group Policy Dialog Box



Step 3 Enter the name of the new group policy in the name field.

The group policy name is *web1* in our example.

Step 4 From the Server Group menu, choose the AAA authorization server group you created previously.

In our example, this is the server group named ldap-authorize.

Step 5 Click **OK** and then **Apply** to create the new group policy.

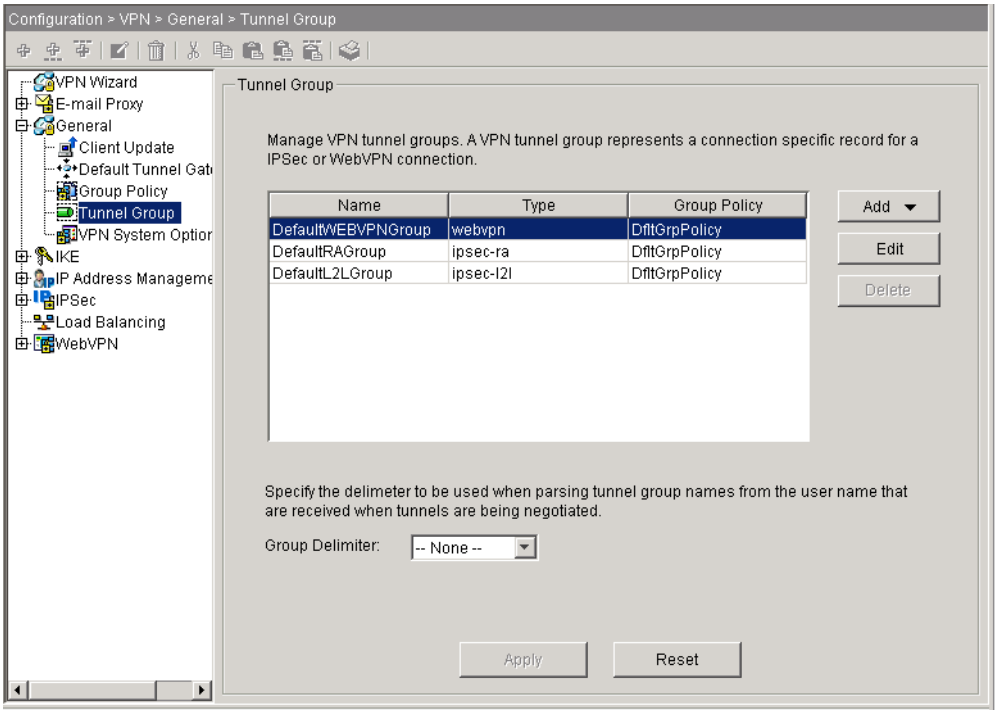
Configuring a Tunnel Group for LDAP Authentication

In the final major task, you create a tunnel group that specifies LDAP authentication by performing the following steps:

Step 1 In the Cisco ASDM window, select **Configuration > VPN > General > Tunnel Group.**

The Tunnel Group area appears on the right side of the ASDM window as shown in Figure 6-9.

Figure 6-9 Tunnel Group Area



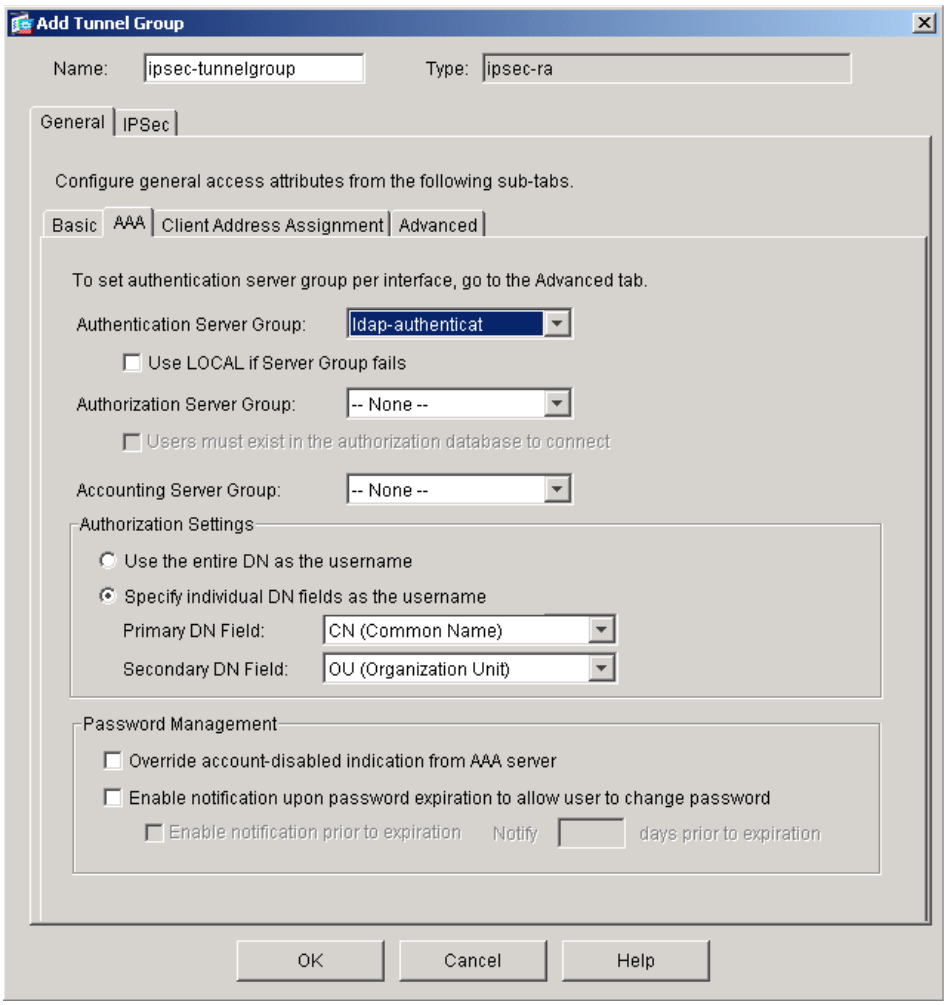
Step 2 Click **Add** in the tunnel Group area and choose the type of tunnel group.

In our example, we choose IPSec for Remote Access.

The Add Tunnel Group dialog box appears.

Step 3 Choose the **General** tab, and then choose the **AAA** tab, as shown in Figure 6-10.

Figure 6-10 Add Tunnel Group Dialog Box with General and AAA Tabs Selected



Step 4 Enter the name of the tunnel group in the Name field.

In our example, the tunnel group name is ipsec-tunnelgroup.

Step 5 From the Authentication Server Group menu, chose the AAA server group you configured for authentication.

In our example, the authentication server group name is ldap-authenticat.

Step 6 Click **OK** at the bottom of the Add Tunnel Group dialog box.

Step 7 Click **Apply** at the bottom of the ASDM window to include the changes to the running configuration.

You have completed this example of the minimal steps required to configure the security appliance for LDAP authentication and authorization.

Configuring Citrix MetaFrame Services

WebVPN users can use a connection to the security appliance to access Citrix MetaFrame services. The following sections introduce this function, list the prerequisites, and describe how to use ASDM to configure the security appliance to support this function:

Note As you follow the instructions in this chapter, click **Help** for more information about the attributes shown in the ASDM windows.

Introduction

The security appliance lets Citrix Independent Computing Architecture (ICA) clients access corporate enterprise applications running on a Citrix Presentation Server over a WebVPN connection. You can redirect the WebVPN home page to the Citrix web server, add a link to the server on the WebVPN home page, or instruct users to enter the URL of the server to access Citrix MetaFrame services. When a WebVPN user connects to the Citrix web server, the Citrix Web Interface authenticates the user and lets the user access corporate resources.

Note Within this configuration, the security appliance functions as the Citrix secure gateway.

Complete the instructions in the following sections to configure security appliance support for Citrix MetaFrame services running on one or more Citrix Presentation Servers.

Before You Begin

Before following the instructions in this chapter, configure the Citrix Web Interface software to operate in a mode that does not use the Citrix secure gateway.

Note All browsers connecting to the Citrix server must support 128-bit encryption.

Adding a Trustpoint

These instructions describe how to add a trustpoint to the security appliance appliance configuration to satisfy a Citrix connection requirement.

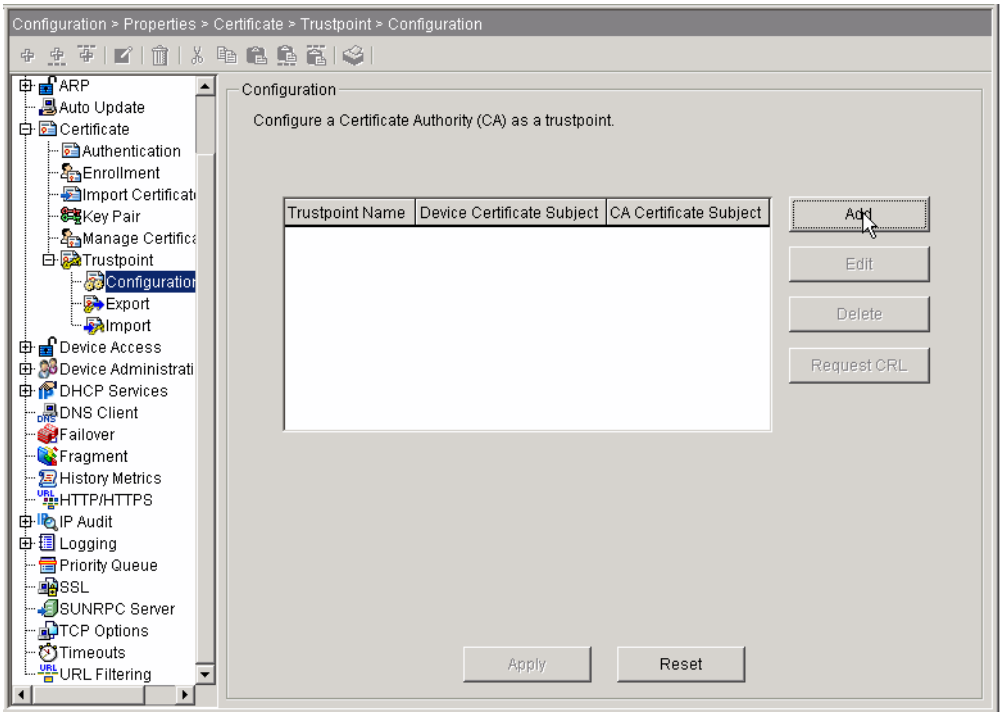
A trustpoint contains the identity of a certificate authority, CA-specific configuration parameters, and an association with one enrolled identity certificate. You need one trustpoint to connect with the Citrix server. You can configure up to two trustpoints, each to be assigned to a different interface on the security appliance; however, you can assign a single trustpoint to two interfaces.

Add a trustpoint to the security appliance configuration as follows:

Step 1 Choose Configuration > Properties > Certificate > Trustpoint > Configuration.

The Trustpoint Configuration window opens (Figure 7-1).

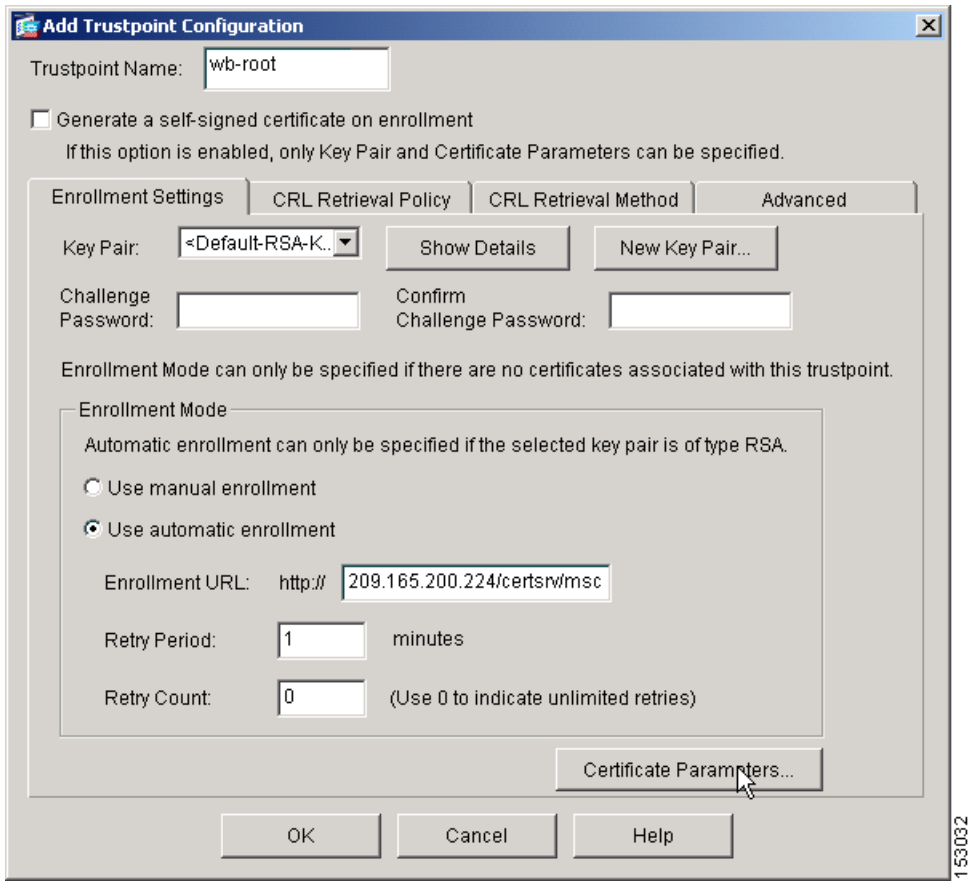
Figure 7-1 Trustpoint Configuration



Step 2 Click **Add**.

The Add Trustpoint Configuration window opens (Figure 7-2).

Figure 7-2 Add Trustpoint Configuration



Step 3 Enter a value, such as the name of the certificate, in the **Trustpoint Name** field to uniquely identify this trustpoint and provide a visual association to the certificate.

Step 4 Click either of the following attributes:

- **Use manual enrollment**

  This option specifies the intention to generate a PKCS10 certification request. The CA issues a certificate to the security appliance based on the request, and the certificate is installed on the security appliance by importing the new certificate.

- **Use automatic enrollment**

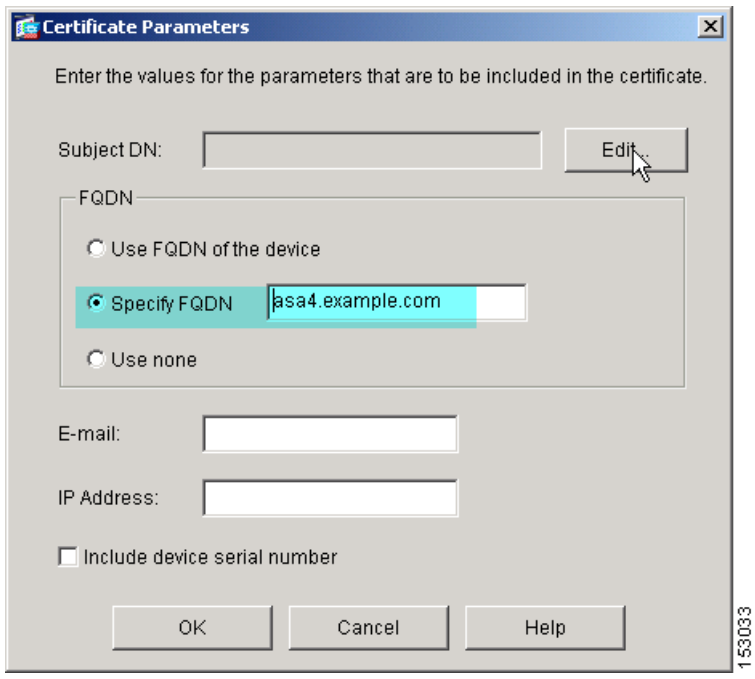
  If you choose this option, Enter the URL for automatic enrollment in the **Enrollment URL** field.

  The automatic enrollment option specifies the intention to use SCEP mode. When the trustpoint is configured for SCEP enrollment, the security appliance downloads the certificate using the SCEP protocol.

Step 5 Click **Certificate Parameters**.

The Certificate Parameters window opens (Figure 7-3).

Figure 7-3 Certificate Parameters



Step 6 Click **Specify FQDN**.

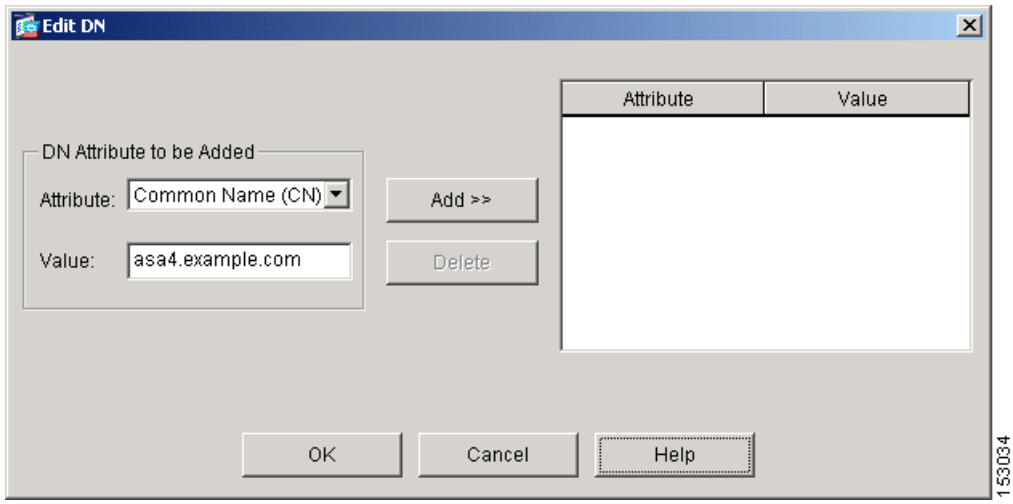
Step 7 Enter the fully qualified domain name used in the Subject Alternative Name extension of the certificate into the **Specify FQDN** field.

The FQDN addresses the server program to which to send requests.

Step 8 Click **Edit**.

The Edit DN window opens (Figure 7-4).

Figure 7-4 Edit DN



Step 9 Select **Common Name** from the drop-down list next to the **Attribute** field.

Step 10 Enter the FQDN you entered in Step 6 into the **Value** field and click **Add**.

The Citrix ICA connection application requires a fully qualified domain name (FQDN) in the common name (CN) field of the SSL certificate.

Caution Do not specify an IP address as the CN.

ASDM inserts the new entry into the table on the right.

Step 11 Click **OK** three times.

ASDM inserts the new trustpoint into the Trustpoint Configuration table (Figure 7-1).

Step 12 Click **Apply** to save the trustpoint to the Flash device.

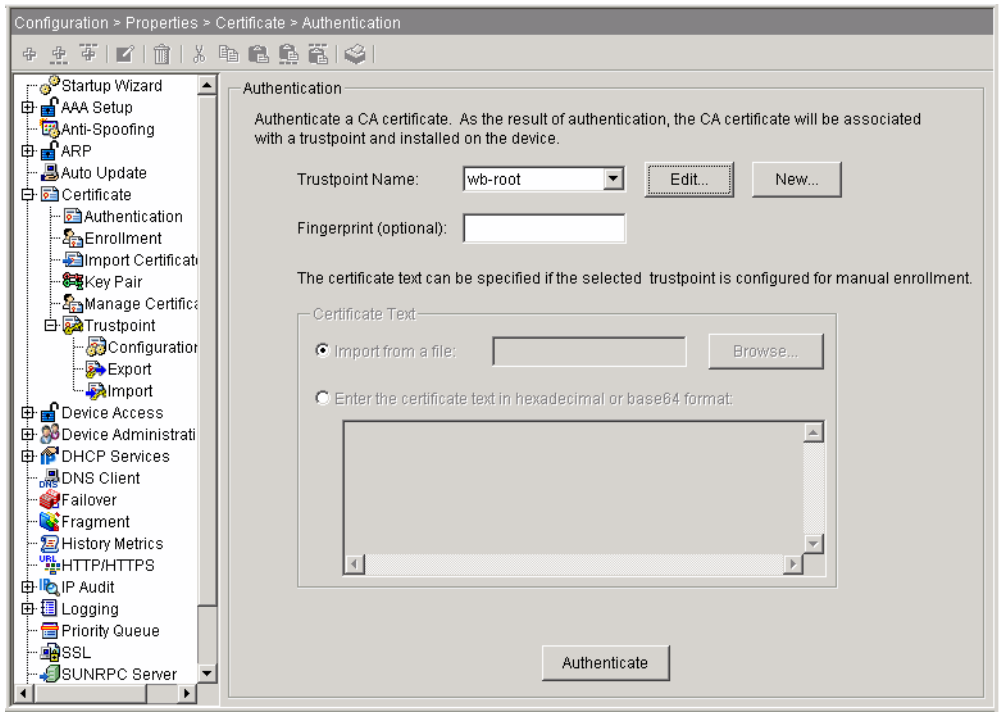
Authenticating the Certificate Authority

Now that you have a trustpoint, you need to authenticate the certificate authority, as follows:

Step 1 Choose Configuration > Properties > Certificate > Authentication.

The Authentication window opens (Figure 7-5).

Figure 7-5 Authentication



Step 2 Select the trustpoint you created in the previous section from the drop-down list next to the **Trustpoint Name** attribute.

Step 3 Click **Authenticate**.

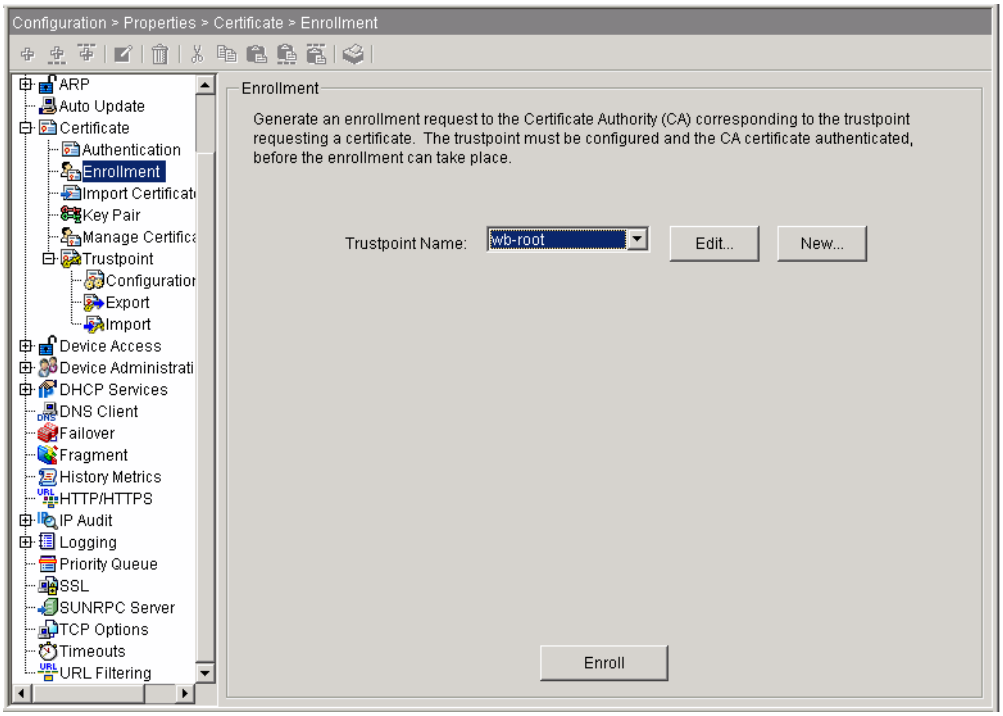
Enrolling the Certificate

When you enroll the certificate, you identify the certificate to be associated with the trustpoint. Enroll the certificate to be used for Citrix connections, as follows:

Step 1 Choose Configuration > Properties > Certificate > Enrollment.

The Enrollment window opens (Figure 7-6).

Figure 7-6 Enrollment



Step 2 Select the trustpoint you created in the previous section from the drop-down list next to the **Trustpoint Name** attribute.

Step 3 Click **Enroll**.

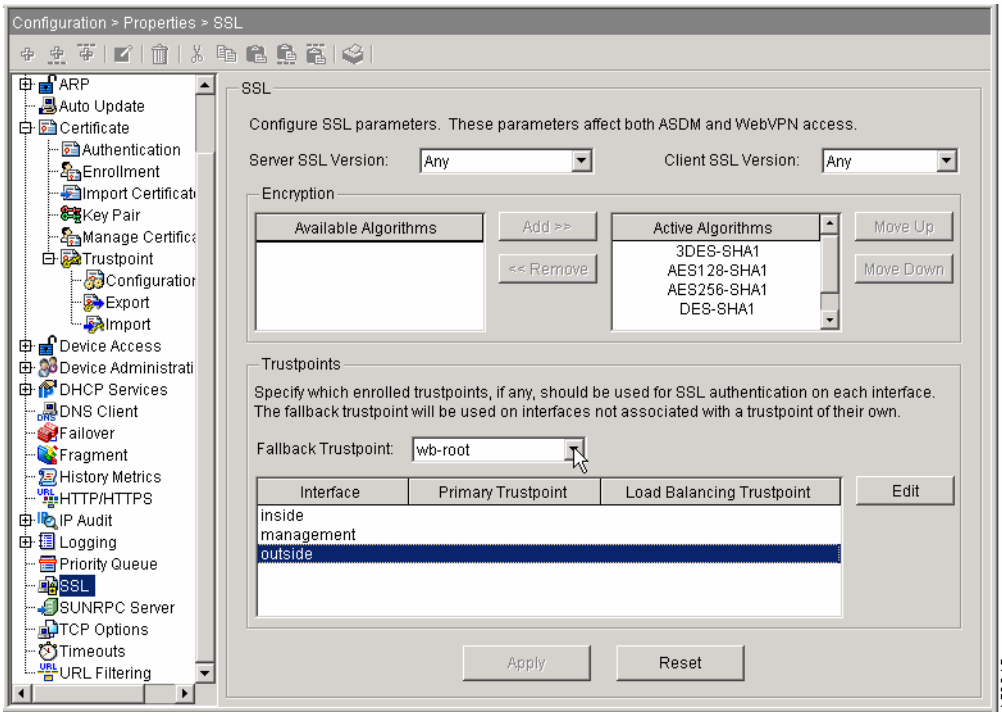
Applying the Trustpoint to an Interface

These instructions describe how to apply the trustpoint to the security appliance interface to be used to terminate WebVPN sessions to the Citrix server. You can, but are not required, to use this interface exclusively for Citrix connections. Apply the trustpoint to the interface as follows:

Step 1 Choose Configuration > Properties > SSL.

The SSL window opens (Figure 7-7).

Figure 7-7 SSL



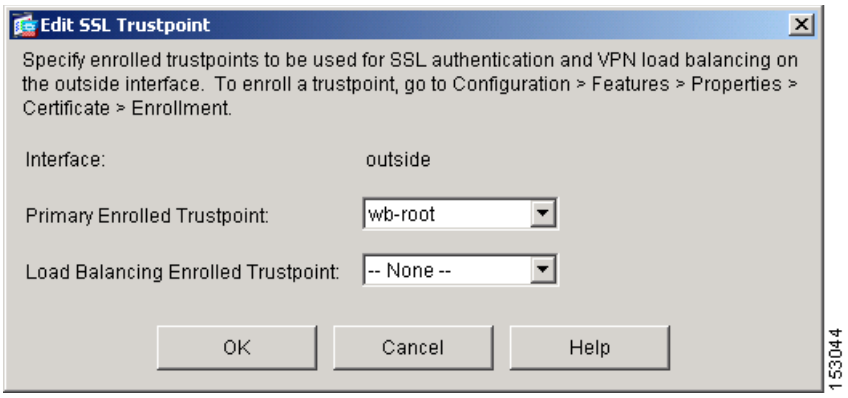
Step 2 Do either of the following:

- Select the trustpoint next to the **Fallback Trustpoint** attribute if you want any interface to use the trustpoint if it doesn't have a specific trustpoint assigned, then click **Apply** to save the configuration change to the Flash device. This step completes the assignment of the trustpoint to the interface.
- Double-click the interface to be used to terminate WebVPN sessions to the Citrix server, to make an explicit assignment of the trustpoint to the interface.

  Typically, the interface used to terminate these sessions is the outside interface.

  The Edit SSL Trustpoint window opens (Figure 7-8).

Figure 7-8 Edit SSL Trustpoint



Step 3 Select the trustpoint next to the **Primary Enrolled Trustpoint** attribute and click **OK**, then click **Apply** to save the configuration change to the Flash device.

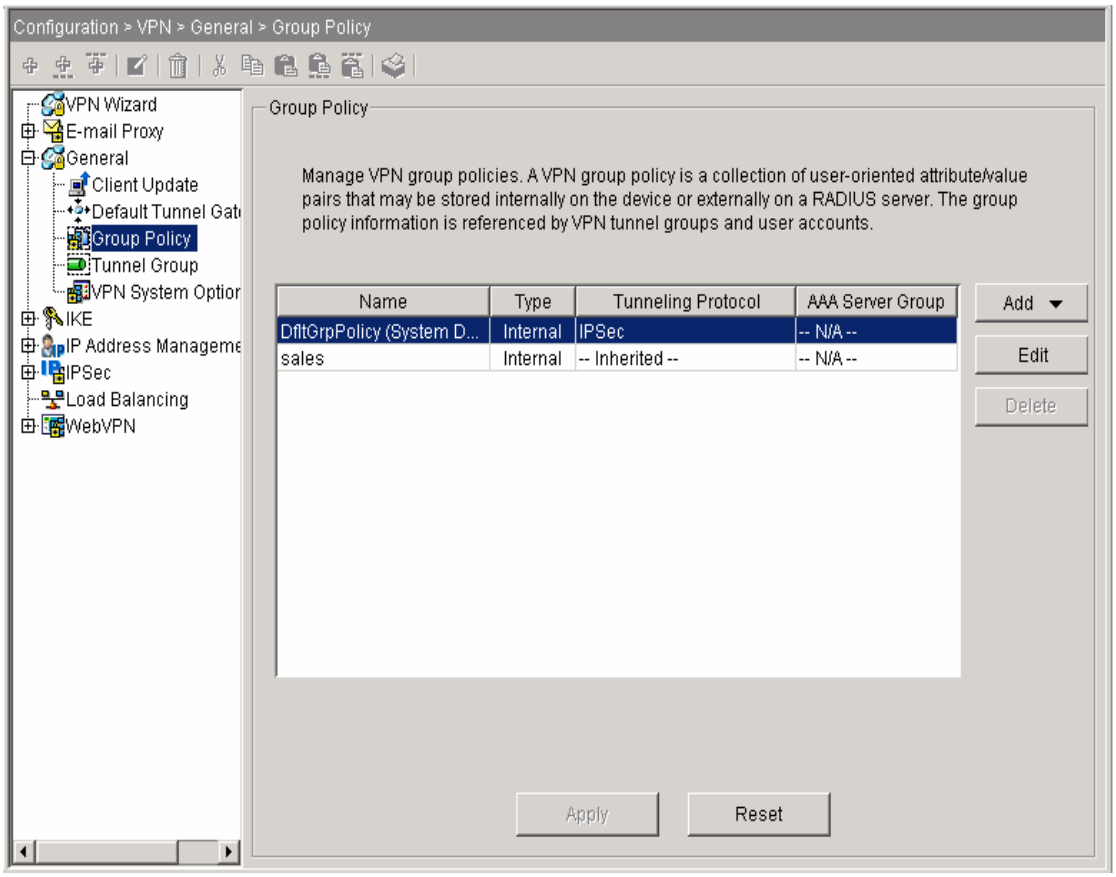
Enabling WebVPN

Remote access to Citrix MetaFrame services requires WebVPN tunneling to be enabled. Enable WebVPN on the group policy applied to the users for whom you want to provide these services as follows:

Step 1 Choose Configuration > VPN > General > Group Policy.

The Group Policy window opens (Figure 7-9).

Figure 7-9 Group Policy



Step 2 Use one of the following strategies:

- Set the default group policy to enable WebVPN tunneling.

  By default, group policies and users inherit the settings of the default group policy.

  Double-click the DfltGrpPolicy entry in the Group Policy table, verify the General tab is open, check **WebVPN** next to Tunneling Protocols, and click **OK**.

- Limit WebVPN to alternative group policies for which you want to provide Citrix MetaFrame services.

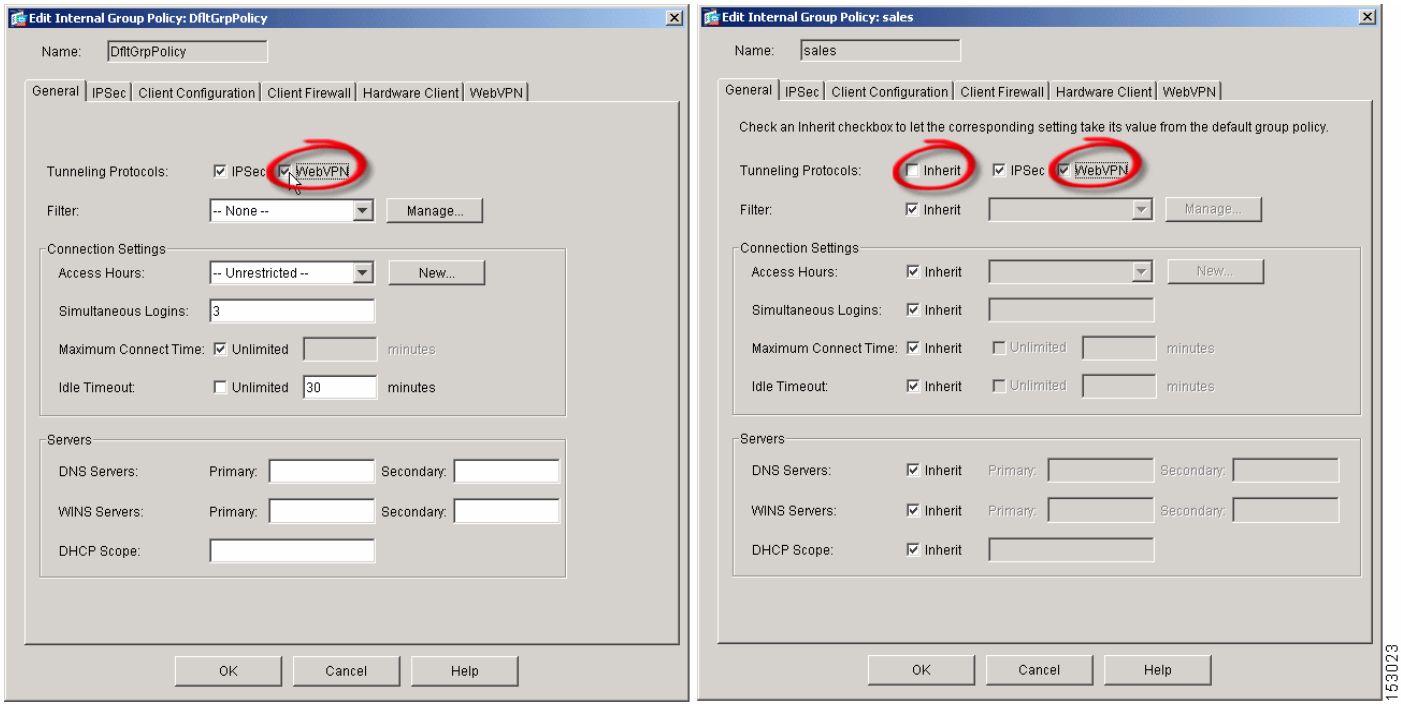
  By default, users inherit the tunneling protocols from their assigned group policies.

  For each internal or external group policy for which you want to provide access to Citrix MetaFrame services, double-click the policy in the Group Policy table, verify the General tab is open, clear the **Inherit** check box next to Tunneling Protocols, check **WebVPN**, and click **OK**.

Note You can also create a new group policy to enable WebVPN services, but if you do, you also need to assign the group policy to the users to whom you want to grant this access right. For more information about configuring group policies, see Chapter 2, "Configuring Group Policies"

Figure 7-10 compares the General tab in the DfltGrpPolicy to that of alternative policies.

Figure 7-10 WebVPN Option in the DfltGrpPolicy and an Alternative Group Policy



Note If you check the Inherit check box in an alternative group policy, the policy uses the WebVPN setting of the default group policy. Clearing the Inherit check box allows you to customize an alternative group policy's WebVPN setting, making it independent from the default group policy's WebVPN setting.

Step 3 Click **Apply** to save the modified group policies to the Flash device.

Enabling Citrix

You can enable Citrix MetaFrame services in the default group policy, alternative group policies, or individual user accounts. Refer to the section that names the strategy you prefer to use.

- Enabling Citrix on a Group Policy, page 7-11
- Enabling Citrix on a User Account, page 7-12

Enabling Citrix on a Group Policy

Enable Citrix MetaFrame services on one or more group policies, as follows:

Step 1 Choose Configuration > VPN > General > Group Policy.

The Group Policy window opens.

Step 2 Use one of the following strategies to enable Citrix MetaFrame services:

- Set the default group policy to enable Citrix.

  By default, alternative group policies and users inherit the settings of the default group policy.

  Double-click the DfltGrpPolicy entry in the Group Policy table, open the **WebVPN > Functions** tab, check **Enable Citrix MetaFrame**, and click **OK**.

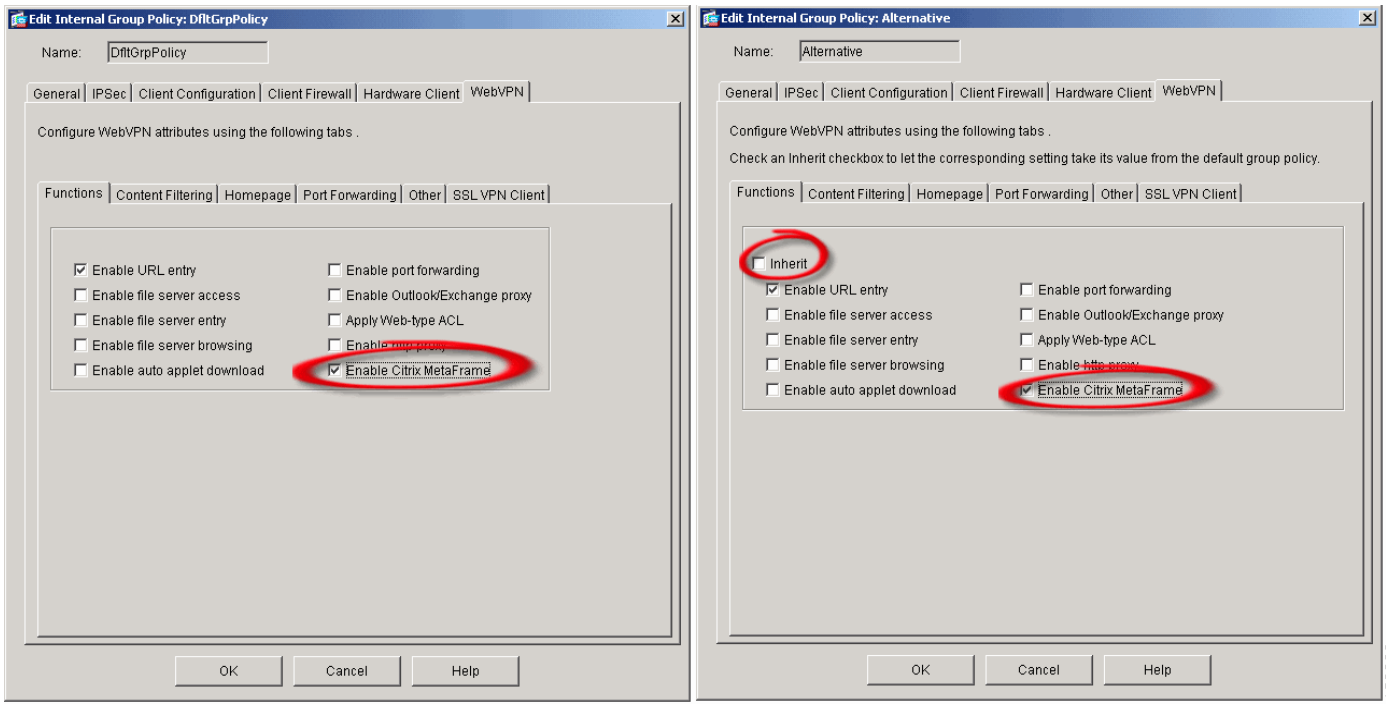
- Set the alternative group policies for which you want to configure support for Citrix to enable WebVPN tunneling.

  By default, users inherit the Functions settings from their respective assigned group policies.

  For each internal or external group policy for which you want to enable Citrix access, double-click the policy in the Group Policy table, open the **WebVPN > Functions** tab, clear **Inherit**, check **Enable Citrix MetaFrame**, and click **OK**.

Figure 7-11 compares the WebVPN > Functions tab in the DfltGrpPolicy to that of alternative policies.

Figure 7-11 Enable Citrix MetaFrame in the DfltGrpPolicy and an Alternative Group Policy



If you check the Inherit check box in an alternative group policy, the policy uses the Enable Citrix MetaFrame of the default group policy. Clearing the Inherit check box allows you to customize an alternative group policy's Functions settings, making them independent from the default group policy's WebVPN setting.

Tip The URL Enable entry attribute shown in Figure 7-11, if checked, lets remote users type the URL of the Citrix server in the WebVPN home page or floating toolbar. Redirecting the home page to the Citrix server or creating a link to the home page and floating toolbar are other ways you can let users connect to the Citrix server. By default, the URL Enable entry attribute is checked in the default group policy. ASDM automatically inserts a check mark to enable this attribute if you clear Inherit in an alternative group policy. Use the default setting (checked) if you want to let users enter URLs, including the URL of the Citrix server. Otherwise, clear this attribute. The section, Configuring a Citrix Access Method, page 7-15, provides more information about the options available to provide WebVPN access to a Citrix server.

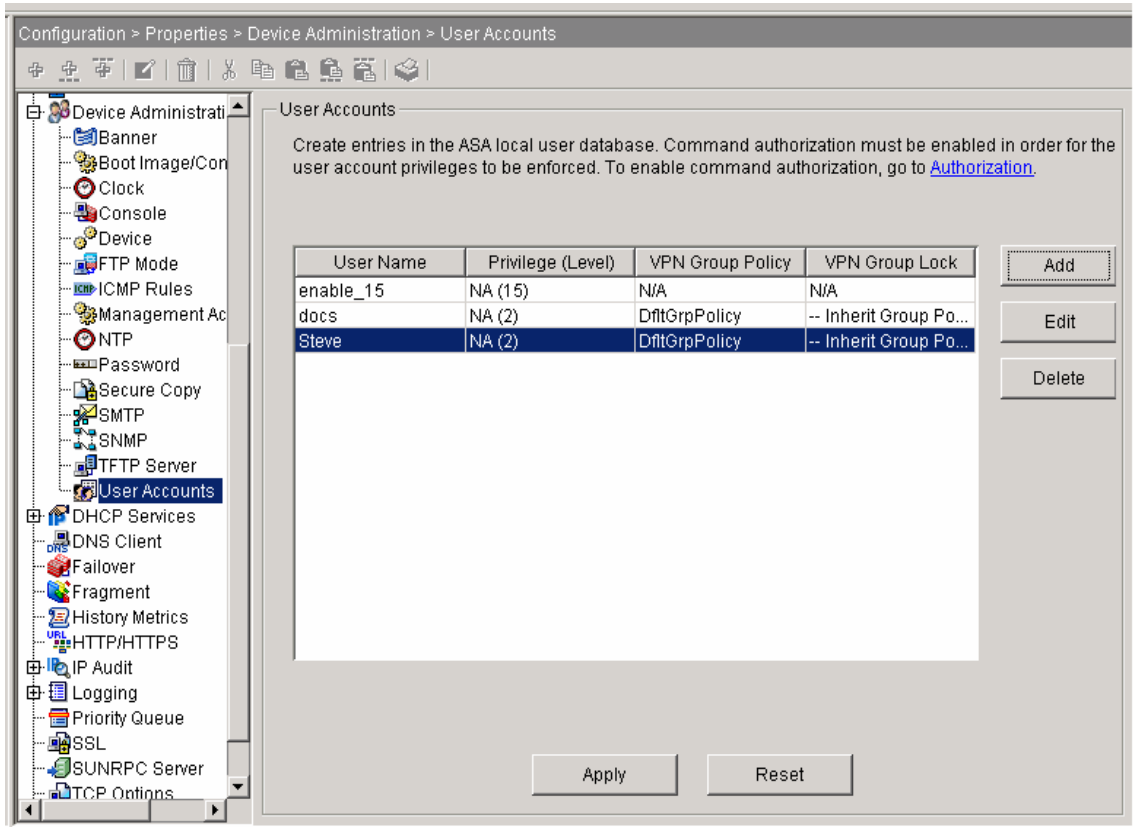
Enabling Citrix on a User Account

As an alternative to enabling Citrix services on group policies applied to users, you can modify user accounts to support Citrix MetaFrame Services. Follow this procedure once for each user account you want to modify.

Step 1 Choose Configuration > Properties > Device Administration > User Accounts.

The User Accounts window opens (Figure 7-12).

Figure 7-12 User Accounts

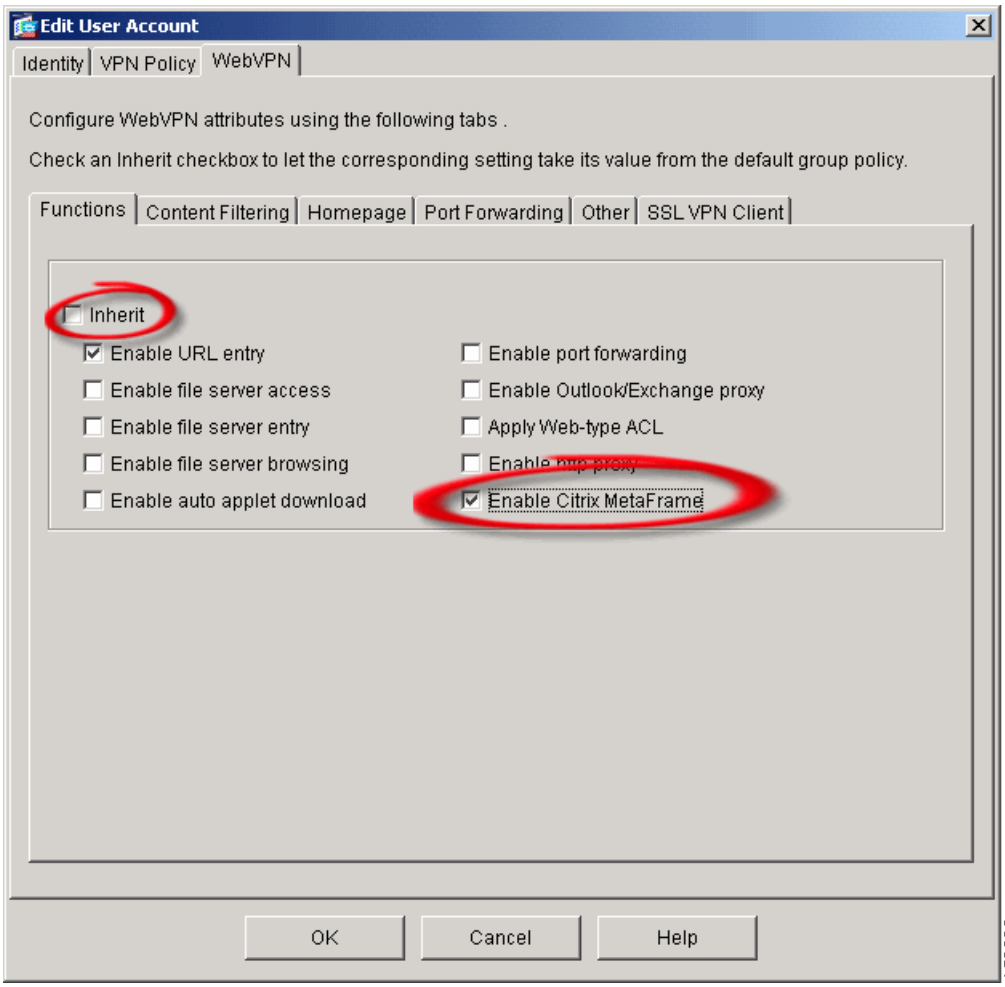


Step 2 Double-click the user name.

Step 3 Open the WebVPN > Functions tab.

The WebVPN Functions window opens (Figure 7-13).

Figure 7-13 Edit User Account — WebVPN Functions



Step 4 Clear the **Inherit check box** and check **Enable Citrix MetaFrame**.

If you check the Inherit check box, the user account uses all of its Functions settings from the assigned group policy. Clearing the Inherit check box lets you customize the Functions settings for that user.

Step 5 Make sure that the other Functions settings are appropriate for the user.

Tip The URL Enable entry attribute shown in Figure 7-13, if checked, lets the user type the URL of the Citrix server in the WebVPN home page or floating toolbar. Redirecting the home page to the Citrix server or creating a link to the home page and floating toolbar are other ways you can let users connect to the Citrix server. By default, the URL Enable entry attribute is checked in the default group policy. ASDM automatically inserts a check mark to enable this attribute if you clear the Inherit check box in the user account. Use the default setting (checked) if you want to let the user enter URLs, including the URL of the Citrix server. Otherwise, clear this attribute. The section, Configuring a Citrix Access Method, page 7-15, provides more information about the options available to provide WebVPN access to a Citrix server.

Step 6 Click **OK**.

Step 7 Click **Apply** to save the modified user accounts to the Flash device.

Note Now that you have cleared the Inherit check box for the Functions settings, the user may lose access to features that were enabled. To view the previously inherited Functions settings, open the **VPN Policy** tab and note the Group Policy setting. Choose Configuration > VPN > General > Group Policy, double-click the group policy name that matches the Group Policy setting you previously viewed, and view the settings in the group policy's **WebVPN > Functions** tab.

Configuring a Citrix Access Method

To let users connect to a Citrix MetaFrame server, they need a facility for doing so on the WebVPN home page or toolbar. To provide a means to connect to the Citrix server, refer to the section that names the method you want to use.

- Redirecting the WebVPN User Home Page to the Citrix Server, page 7-15
- Adding a Link on the WebVPN Home Page to the Citrix Server, page 7-17
- Enabling URL Entry on the WebVPN Home Page, page 7-25

Redirecting the WebVPN User Home Page to the Citrix Server

To let WebVPN users access a Citrix server, you can specify its URL as the remote user's WebVPN home page. Use at least one of the following sections to change the URL of the home page:

- Redirecting the Home Page on a Group Policy, page 7-15
- Redirecting the Home Page on a User Account, page 7-16

Redirecting the Home Page on a Group Policy

Redirect the WebVPN home page to the URL of a Citrix MetaFrame server in one or more group policies, as follows:

Step 1 Choose Configuration > VPN > General > Group Policy.

The Group Policy window opens.

Step 2 Use one of the following strategies to redirect the WebVPN home page:

- Set the default group policy to redirect the WebVPN home page.

  By default, alternative group policies and users inherit the Custom Homepage setting of the default group policy.

  Double-click the DfltGrpPolicy entry in the Group Policy table, open the **WebVPN > Homepage** tab, click **Specify URL**, select **http** from the drop-down menu, enter the URL of the Citrix server in the field to the right, and click **OK**.

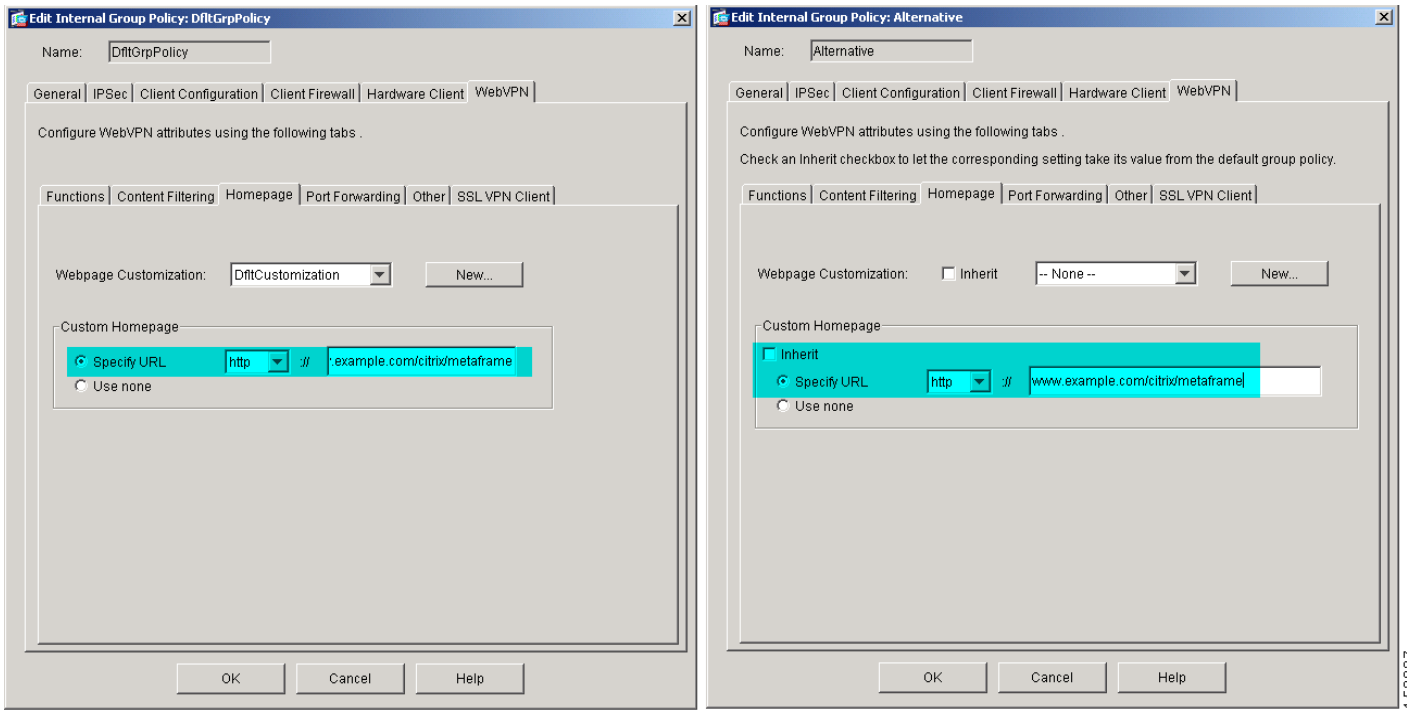
- Set the alternative group policies to redirect the WebVPN home page.

  By default, users inherit the Custom Homepage setting from their respective assigned group policies.

For each internal or external group policy for which you want to redirect the WebVPN home page, double-click the policy in the Group Policy table, open the **WebVPN > Homepage** tab, clear **Inherit** in the Custom Homepage area, click **Specify URL**, select **http** from the drop-down menu, enter the URL of the Citrix server in the field to the right, and click **OK**.

Figure 7-14 compares the WebVPN > Homepage tab in the DfltGrpPolicy to that of alternative policies.

Figure 7-14 Home Page Redirection in the DfltGrpPolicy and an Alternative Group Policy



Note If you check the Inherit check box in an alternative group policy, the policy uses the Custom Homepage area settings of the default group policy. Clearing the Inherit check box lets you customize the Custom Homepage area settings for an alternative group policy, making those settings independent from those of the default group policy.

Step 3 Click **Apply** to save the modified group policies to the Flash device.

Redirecting the Home Page on a User Account

As an alternative to redirecting the WebVPN home page on group policies, you can redirect it on user accounts. For each user account for which you want to redirect the home page, do the following steps:

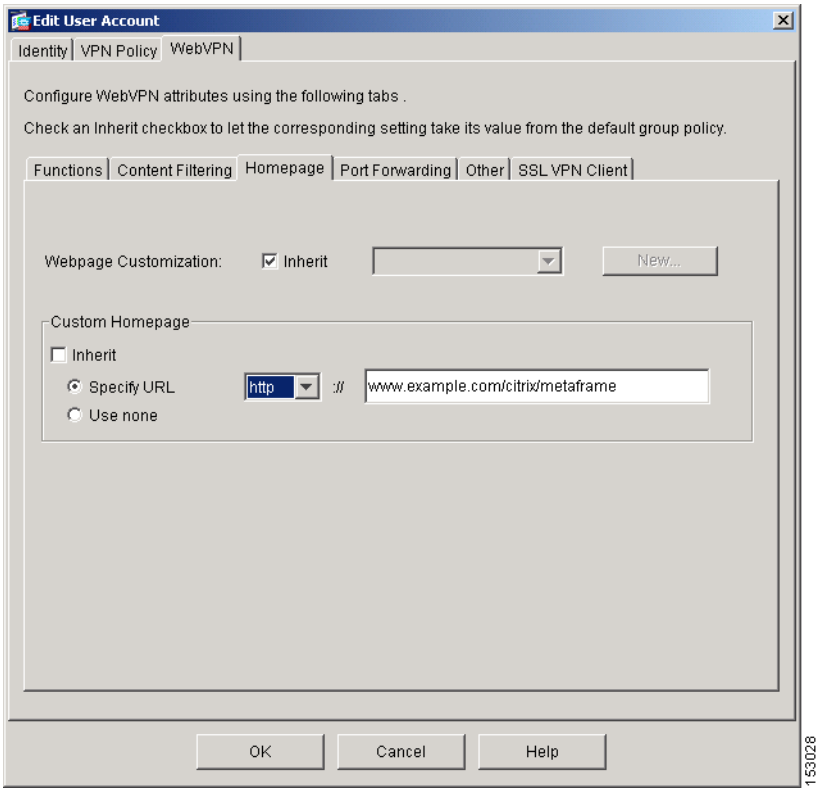
Step 1 Choose Configuration > Properties > Device Administration > User Accounts.

The User Accounts window opens.

Step 2 Double-click the user name and open the **WebVPN > Homepage** tab.

Figure 7-15 shows the Edit User Account WebVPN > Homepage tab.

Figure 7-15 Edit User Account WebVPN > Homepage Tab



Step 3 Clear the **Inherit** check box in the Custom Homepage area, click **Specify URL**, select **http** from the drop-down menu, enter the URL of the Citrix server in the field to the right, and click **OK**.

Note If you check the Inherit check box, the user account uses Custom Homepage settings from the assigned group policy. Clearing the Inherit check box lets you customize the settings for that user.

Step 4 Click **Apply** to save the modified user accounts to the Flash device.

Adding a Link on the WebVPN Home Page to the Citrix Server

To let WebVPN users access a Citrix server, you can display a link to the server on the WebVPN home page and floating toolbar (Figure 7-16).

Figure 7-16 WebVPN Home Page and Floating Toolbar

Users only need to click on the Citrix link in the Web Bookmarks menu or list to access the Citrix server.

Use the instructions in the following sections to prepare and configure the link to the Citrix server.

- Examining the URL List Mappings, page 7-18
- Configuring the Link to the Citrix Server, page 7-20

Examining the URL List Mappings

Inserting a URL onto the WebVPN home page requires modifying one or more existing lists of URLs or adding one or more new lists. (A “list” can consist of only one URL.)

To know which lists to modify or whether to add a new list, you need to know whether the group policies and user accounts for whom you want to create a Citrix link are using a list, and if so, which list. Examine the current group policy and user account configuration to determine how to proceed, as follows:

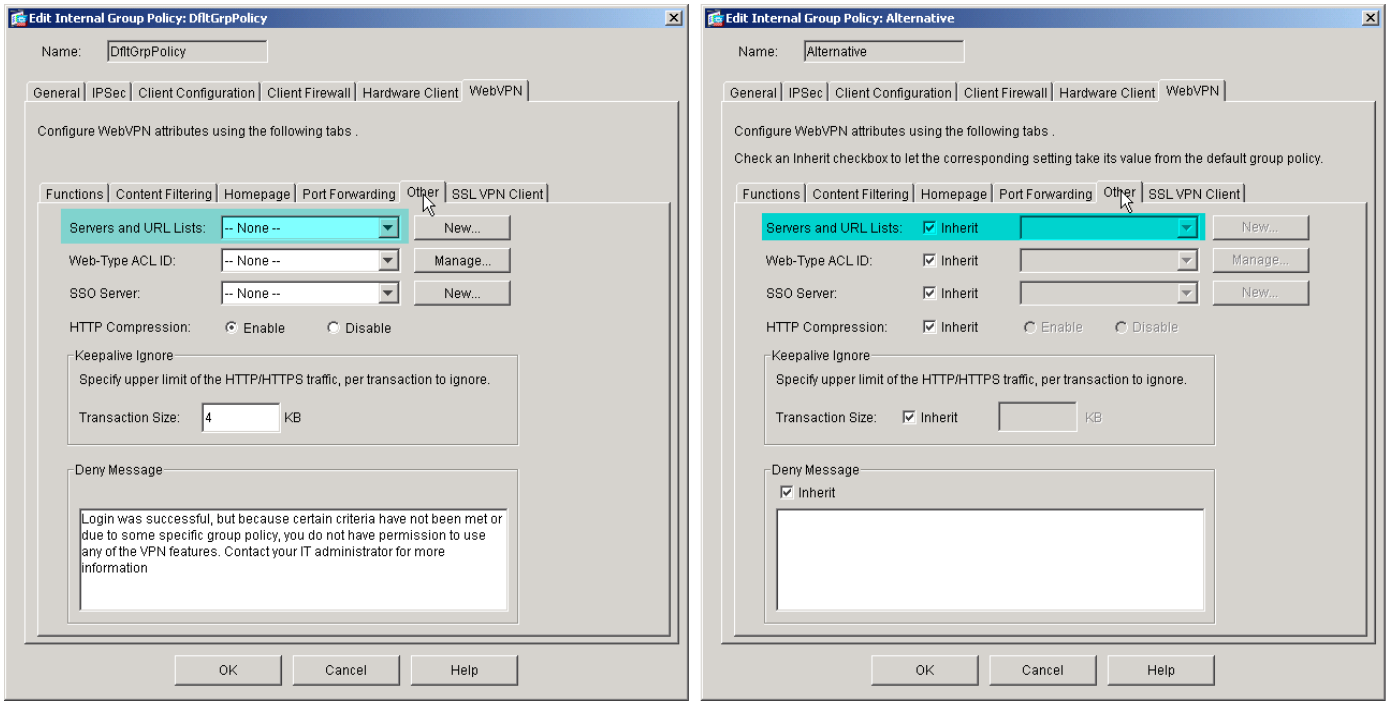
Step 1 Choose Configuration > VPN > General > Group Policy.

The Group Policy window opens.

Step 2 For each group policy, double-click the policy name and open the **WebVPN** > **Other** tab.

Figure 7-17 compares the WebVPN > Other tab of the default group policy to that of the alternative policy.

Figure 7-17 Servers and URL Lists in the DfltGrpPolicy and an Alternative Group Policy



Step 3 Note the values of the Servers and URLs Lists attributes, then click **Cancel**.

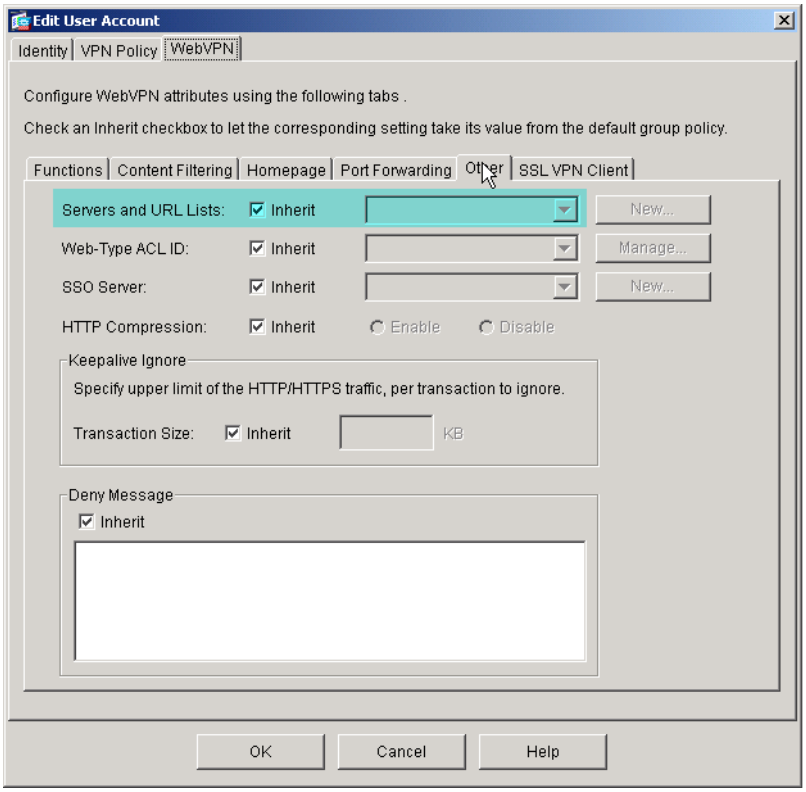
Step 4 Choose Configuration > Properties > Device Administration > User Accounts.

The User Accounts window opens.

Step 5 For each user account for which you are adding support for Citrix services, double-click the policy name and open the **WebVPN > Other** tab.

Figure 7-18 shows the Servers and URL Lists attributes on the WebVPN > Other tab of an example user account.

Figure 7-18 Servers and URL Lists Attribute in a User Account



Step 6 Note the values of the Servers and URLs Lists attributes, then click **Cancel**.

Configuring the Link to the Citrix Server

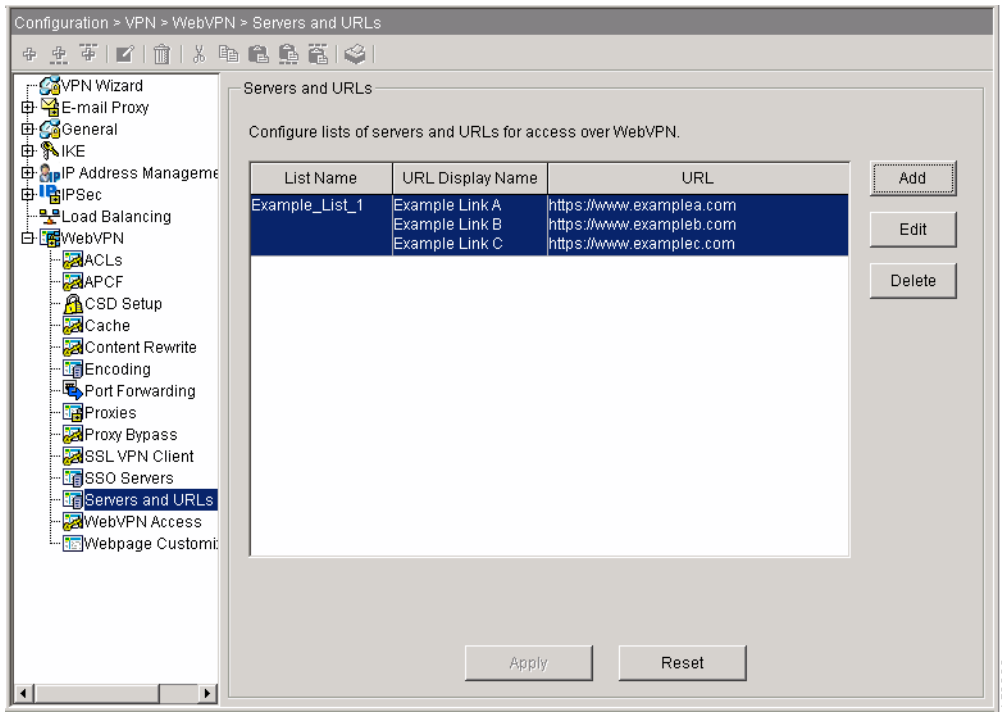
Now that you know whether the group policies and users for whom you want to provide Citrix MetaFrame services are using URL lists, and the names of any URL lists they are using, you are qualified to modify the security appliance configuration of servers and URLs to create the link to the Citrix server.

Create the link to the Citrix server and assign it to the group policies and users for whom you are configuring Citrix access, as follows:

Step 1 Choose Configuration > VPN > WebVPN > Servers and URLs.

The Servers and URLs window opens (Figure 7-19).

Figure 7-19 Servers and URLs



Each list displayed in this window consists of the link names (URL Display Names) and their associated URLs. Following the configuration of a new list, you assign it to at least one group policy or user account to display the list on the WebVPN home page and floating toolbar.

If you add a link to a list that is already assigned to a group policy or user account, the WebVPN home page and floating toolbar automatically add the link for each subsequent login.

Note The Servers and URLs lists have a one-to-one association with the default group policy, and a one-to-many relationship to alternative group policies and user accounts. You can assign one list to more than one group policy and user account, but you cannot assign more than one list to the same group policy or user account.

Step 2 Continue with the instructions in one of the following sections:

- See Adding a Servers and URLs List, page 7-22 if the group policies or user accounts for which you are configuring Citrix services do not have an assigned Servers and URLs list.
- See Adding a URL to a Servers and URLs List, page 7-23 if the group policies or user accounts for which you are configuring Citrix services already have an assigned Servers and URLs list.

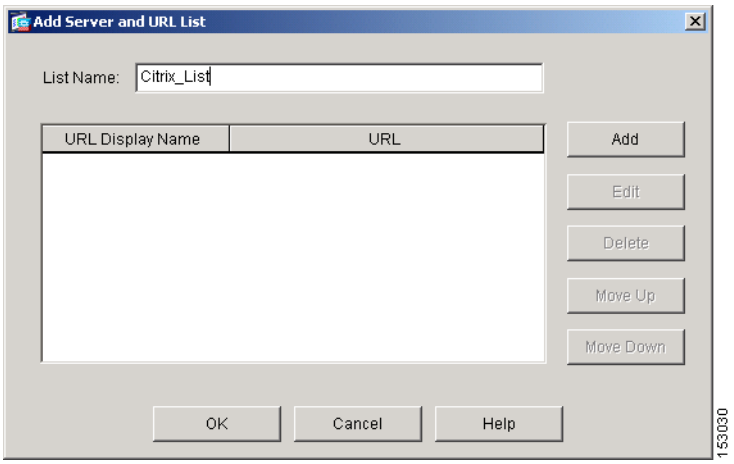
Adding a Servers and URLs List

Continue with the instructions from the previous section to add a Servers and URLs list if the group profiles or user accounts for which you are configuring access to Citrix MetaFrame services do not already have an assigned Servers and URLs list:

Step 1 Click Add in the Servers and URLs window shown in Figure 7-19.

The Add Server and URL List window opens (Figure 7-20)

Figure 7-20 Add Server and URL List

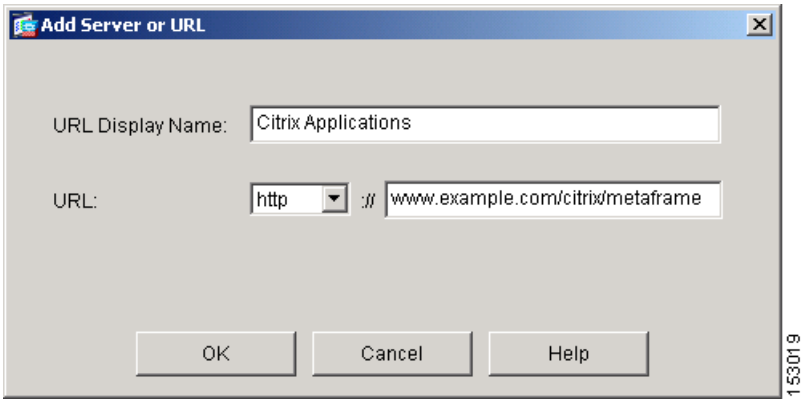


Step 2 Enter a name in the List Name field to differentiate this list from the others in the Servers and URLs configuration. We suggest a name that describes the intent of the group profiles and user accounts for which you want to use them.

Step 3 Click **Add** to create the Citrix link.

The Add Server or URL window opens (Figure 7-21).

Figure 7-21 Add Server or URL



Step 4 Select **http** from the drop-down menu, enter the URL of the Citrix server in the field to the right, and click **OK**.

ASDM inserts the URL entry into the Add Server and URL List table shown in Figure 7-20.

Step 5 Click **OK**.

ASDM inserts the list entry into the Servers and URLs window shown in Figure 7-19.

Step 6 Click **Apply** to save the modified Servers and URLs configuration to the Flash device.

Step 7 Choose Configuration > VPN > General > Group Policy.

The Group Policy window opens.

Step 8 For each group policy for which you want to provide a URL to the Citrix MetaFrame server, double-click the group policy, open the **WebVPN > Other** tab, clear the **Inherit** check box next to Servers and URL Lists if the group policy is an alternative to the default group policy, select the list you created in the drop-down menu to the right of the Servers and URL Lists attribute, and click **OK**.

Step 9 Click **Apply** to save the modified group policies to the Flash device.

Step 10 Choose Configuration > Properties > Device Administration > User Accounts.

The User Accounts window opens.

Step 11 For each custom user account for which you want to provide a URL to the Citrix MetaFrame server, double-click the user account, open the **WebVPN > Other** tab, clear the **Inherit** check box next to the Servers and URL Lists attribute, select the list you created in the drop-down menu to the right of Servers and URL Lists, and click **OK**.

Step 12 Click **Apply** to save the modified user accounts to the Flash device.

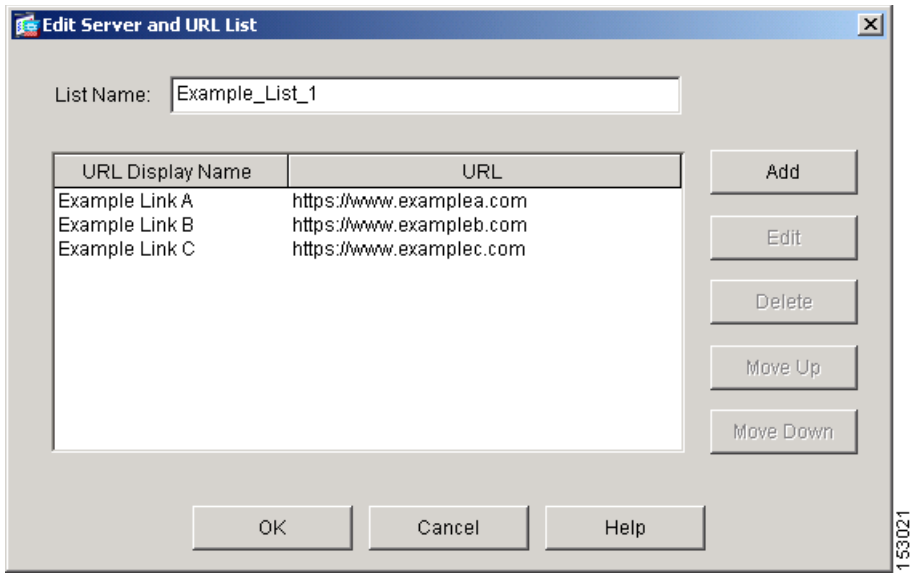
Adding a URL to a Servers and URLs List

Continue with the instructions to modify an entry in the Servers and URLs table displayed in Figure 7-19. Use these instructions only if the group policies or user accounts for which you want to add a URL to the Citrix server already have a Servers and URLs list assignment.

Step 1 Double-click the entry in the Servers and URLs window (Figure 7-19).

The Edit Server and URL List window opens (Figure 7-22)

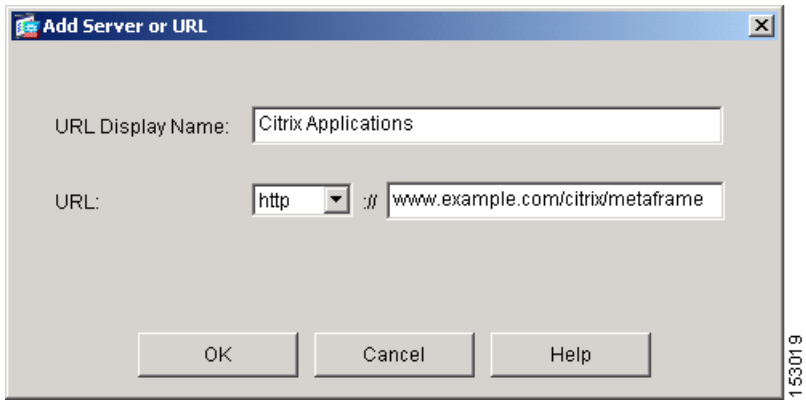
Figure 7-22 Edit Server and URL List



Step 2 Click **Add** to insert the Citrix link into this list.

The Add Server or URL window opens (Figure 7-23).

Figure 7-23 Add Server or URL



Step 3 Select **http** from the drop-down menu, enter the URL of the Citrix server in the field to the right, and click **OK**.

ASDM inserts the URL entry into the Edit Server and URL List table shown in Figure 7-22.

Step 4 Click **OK**.

ASDM inserts the list entry into the Servers and URLs window shown in Figure 7-19.

Step 5 Click **Apply** to save the modified list to the Flash device.

Note This step completes the configuration of the link to the Citrix server if the Servers and URLs list is already assigned to all of the group policies and user accounts for which you want to add a link to the Citrix server. If it is not, continue with the remaining instructions.

Step 6 Choose Configuration > VPN > General > Group Policy.

The Group Policy window opens.

Step 7 For each group policy for which you want to assign the list containing the newly added link to the Citrix server, double-click the group policy, open the **WebVPN > Other** tab, clear the **Inherit** check box next to Servers and URL Lists if the group policy is an alternative to the default group policy, select the list you created in the drop-down menu to the right of Servers and URL Lists, and click **OK**.

Step 8 Click **Apply** to save the modified group policies to the Flash device.

Step 9 Choose Configuration > Properties > Device Administration > User Accounts.

The User Accounts window opens.

Step 10 For each custom user account for which you want to assign the list containing the newly added link to the Citrix server, double-click the user account, open the **WebVPN > Other** tab, clear **Inherit** check box next to Servers and URL Lists, select the list you created in the drop-down menu to the right of Servers and URL Lists, and click **OK**.

Step 11 Click **Apply** to save the modified user accounts to the Flash device.

Enabling URL Entry on the WebVPN Home Page

To let WebVPN users access a Citrix server, you can enable URL entry and send them the URL to enter to access the server. Users enter the URL into the Enter Web Address field of the WebVPN home page or floating toolbar (Figure 7-16).

The default setting of the Enable URL Entry attribute in the default group policy is checked.

The Enable URL Entry attribute in the WebVPN > Functions tab of the group policy or user account, if checked, lets remote users type the URL of the Citrix server in the WebVPN home page or floating toolbar. By default, the Enable URL Entry attribute shown on the left side in Figure 7-11 is checked in the default group policy. ASDM automatically inserts a check mark to enable this parameter if you e Inherit in an alternative group policy or user account. Use the default setting (checked) if you want to let users enter URLs, including the URL of the Citrix server. Otherwise, clear this attribute.

Because the Enable URL Entry attribute is enabled by default, it is unlikely that you will need to do anything to display the Enter Web Address field on the WebVPN home page or floating toolbar. We do, however, recommend that you check the value of this attribute for each group policy and user account to be sure that users can use the Enter Web Address field. Make sure the Enable URL Entry attribute is either checked or inherited from each applicable group policy or user account, as follows:

Step 1 For each group policy for which you enabled Citrix MetaFrame services, choose Configuration > VPN > General > Group Policy, double-click the entry in the Group Policy table (beginning with the DfltGrpPolicy if you are using it for Citrix access), open the **WebVPN > Functions** tab, check **Inherit** or both **Enable URL Entry** and **Enable Citrix MetaFrame**, click **OK**, and click **Apply**.

Step 2 For each user account for which you enabled Citrix MetaFrame services, choose Configuration > Properties > Device Administration > User Accounts, double-click the entry in the User Accounts table, open the **WebVPN > Functions** tab, check **Inherit** or both **Enable URL Entry** and **Enable Citrix MetaFrame**, click **OK**, and click **Apply**.

Configuring Single Sign-on for WebVPN

This chapter presents example procedures for configuring SSO for WebVPN users. It includes the following sections:

Using Single Sign-on with WebVPN

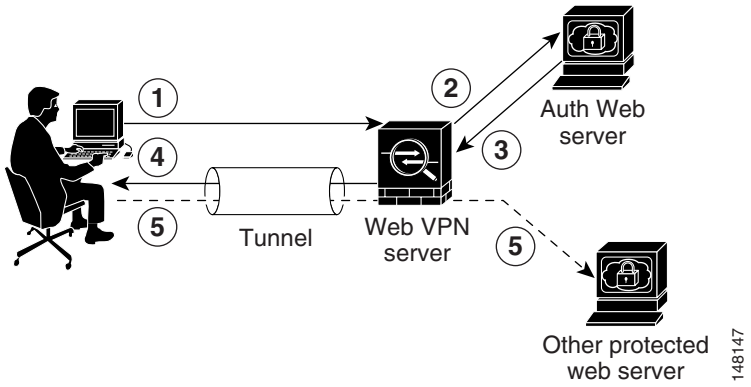
Single sign-on lets WebVPN users enter a username and password only once to access multiple protected services and web servers. In general, the SSO mechanism either starts as part of the AAA process or just after successful user authentication to a AAA server. The WebVPN server running on the security appliance acts as a proxy for the user to the authenticating server. When a user logs in, the WebVPN server sends an SSO authentication request, including username and password, to the authenticating server using HTTPS. If the server approves the authentication request, it returns an SSO authentication cookie to the WebVPN server. The security appliance keeps this cookie on behalf of the user and uses it to authenticate the user to secure websites within the domain protected by the SSO server.

While WebVPN supports three SSO authentication methods, two can be configured with ASDM: SSO with the Computer Associates eTrust SiteMinder server (formerly Netegrity SiteMinder), and SSO using the HTTP Form protocol. The third method, SSO with HTTP Basic and NTLMv1 (NT LAN Manager) authentication, is currently only configurable using the security appliance command line interface.

Figure 8-1 illustrates the following major SSO authentication steps that are used by all three methods:

1. A WebVPN user first enters a username and password to log into the WebVPN server on the security appliance.
2. The WebVPN server acts as a proxy for the user and forwards the form data (username and password) to an authenticating web server.
3. If the authenticating web server approves the user data, it returns an authentication cookie to the WebVPN server where it is stored on behalf of the user.
4. The WebVPN server establishes a tunnel to the user.
5. The user can now access other websites within the protected SSO environment without reentering a username and password.

Figure 8-1 SSO Authentication Using HTTP Forms



Configuring SSO Authentication Using SiteMinder

This section describes configuring the security appliance to support SSO with SiteMinder. You would typically choose to implement SSO with SiteMinder if your website security infrastucture already incorporates SiteMinder. With this method, SSO authentication is separate from AAA and happens once the AAA process completes. If you want to configure SSO for a WebVPN user or group, you must first configure a AAA server, such as a RADIUS or LDAP server. You can then setup SSO support for WebVPN.

This section includes the following topics:

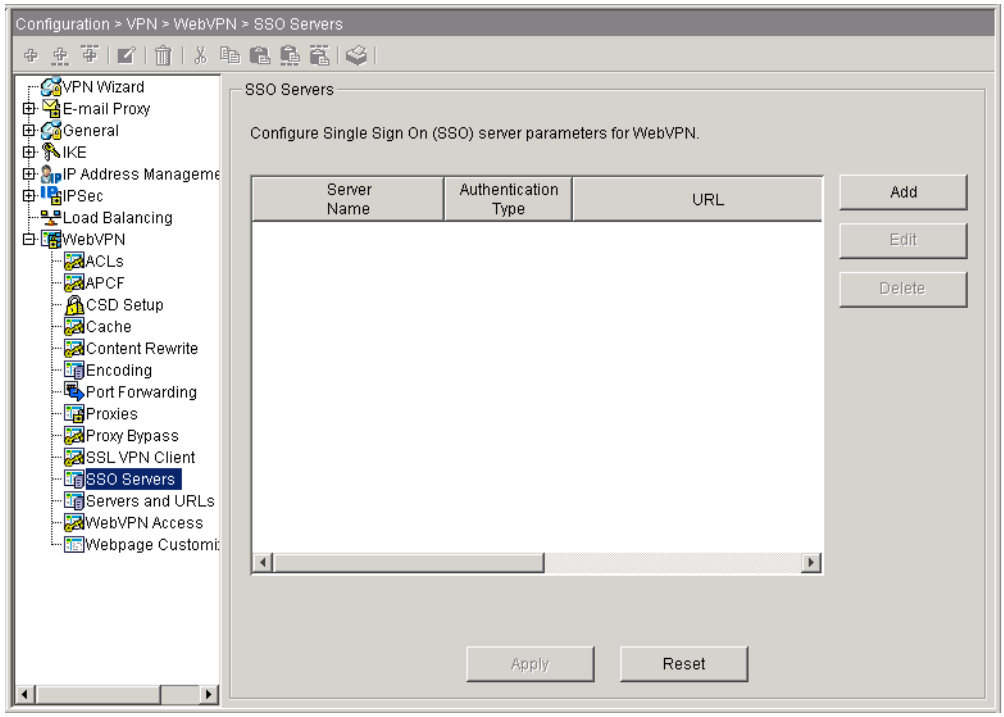
Configuring the Security Appliance for SiteMinder

To configure SSO with a new SiteMinder server, perform the following steps:

Step 1 In the main Cisco ASDM window, choose **Configuration > VPN > WebVPN > SSO Servers**.

The SSO Servers area appears in the window on the right as shown in Figure 8-2.

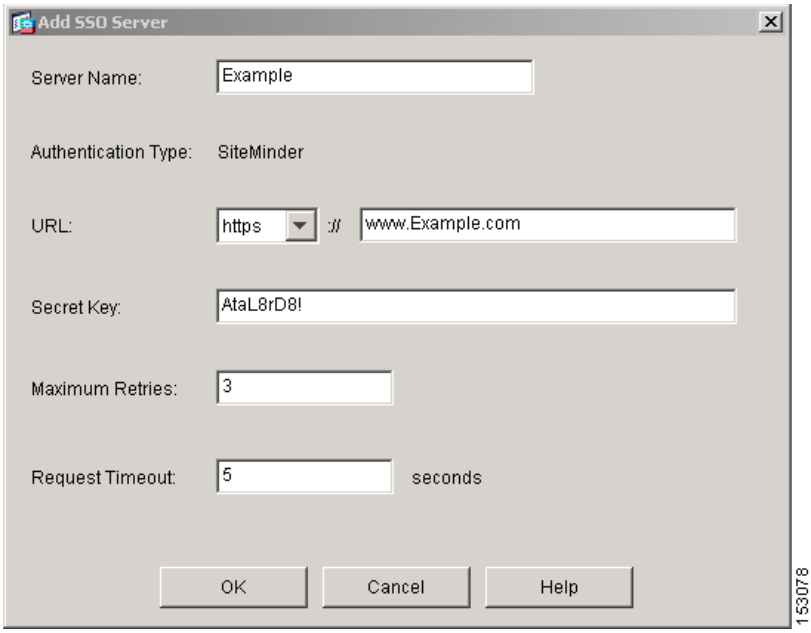
Figure 8-2 ASDM Window with SSO Servers Area Displayed



Step 2 Click **Add** in the SSO Servers area.

The Add SSO Server dialog box appears as shown in Figure 8-3.

Figure 8-3 Add SSO Server Dialog Box



Step 3 In the Server Name field, enter the name of the SiteMinder SSO server.

The minimum number of characters is 4, and the maximum is 31.

In this example, the server name is *Example*.

Step 4 Enter the SSO server URL by performing the following steps:

a. Choose either **HTTP** or **HTTPS** from the menu.

In this example, we choose HTTPS to secure the authentication messages between the security appliance and the SiteMinder server.

b. Enter the rest of the complete server URL.

In this example, the rest of the URL is *www.Example.com*.

This is the SSO server URL to which the security appliance makes SSO authentication requests.

Step 5 Enter the secret key in the Secret Key field.

This is the key used to encrypt authentication communications with the SSO server. The key can be comprised of any regular or shifted alphanumeric character. There is no minimum or maximum number of characters.

The secret key is similar to a password: you create it, save it, and enter it on both the security appliance and the SiteMinder Policy Server. See Adding the Cisco Authentication Scheme to SiteMinder, page 8-9.

In this example, the secret key is AtaL8rD8!.

Step 6 In the Maximum Retries field, enter the number of times the security appliance retries a failed SSO authentication attempt. This step is optional.

The range is 1 to 5 retries, and the default number of retries is 3.

In this example, the maximum retries is 3.

Step 7 In the Request Timeout field, enter the number of seconds before a failed SSO authentication attempt times out. This step is optional.

The range is from 1 to 30 seconds inclusive, and the default is 5 seconds.

In this example, timeout occurs after 5 seconds.

Step 8 Click **OK** to enter this new SSO server in the SSO Server table in the ASDM window.

Step 9 Click **Apply** to add the new SSO server to the running security appliance configuration.

Assigning the SSO Server to Group Policies and Users

After you configure the SSO server, you must specify SSO authentication for either a group policy or a user. This section includes:

- Assigning the SSO Server to a Group Policy, page 8-5
- Assigning the SSO Server to a User, page 8-7

Assigning the SSO Server to a Group Policy

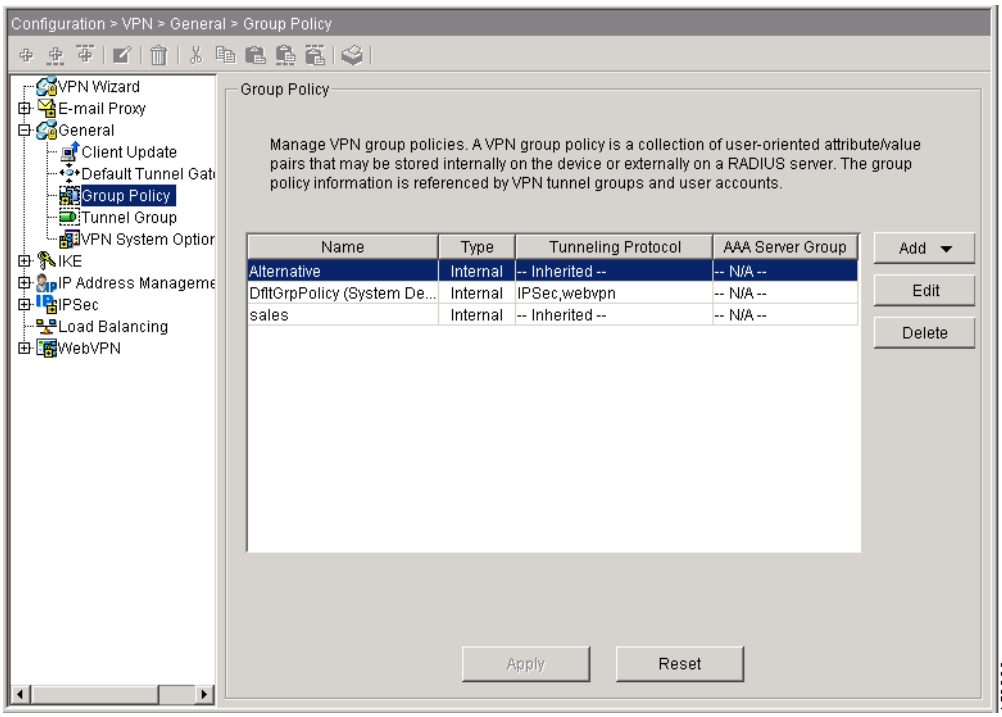
Note Comprehensive procedures for configuring group policies are provided elsewhere in this guide. The following steps are only those that apply to configuring a SiteMinder SSO server.

To assign the SSO server to a group policy, perform the following steps:

Step 1 In the main Cisco ASDM window, choose **Configuration > VPN > General > Group Policy**.

The Group Policy area appears in the window as shown in Figure 8-4.

Figure 8-4 ASDM Window with Group Policy Area Displayed

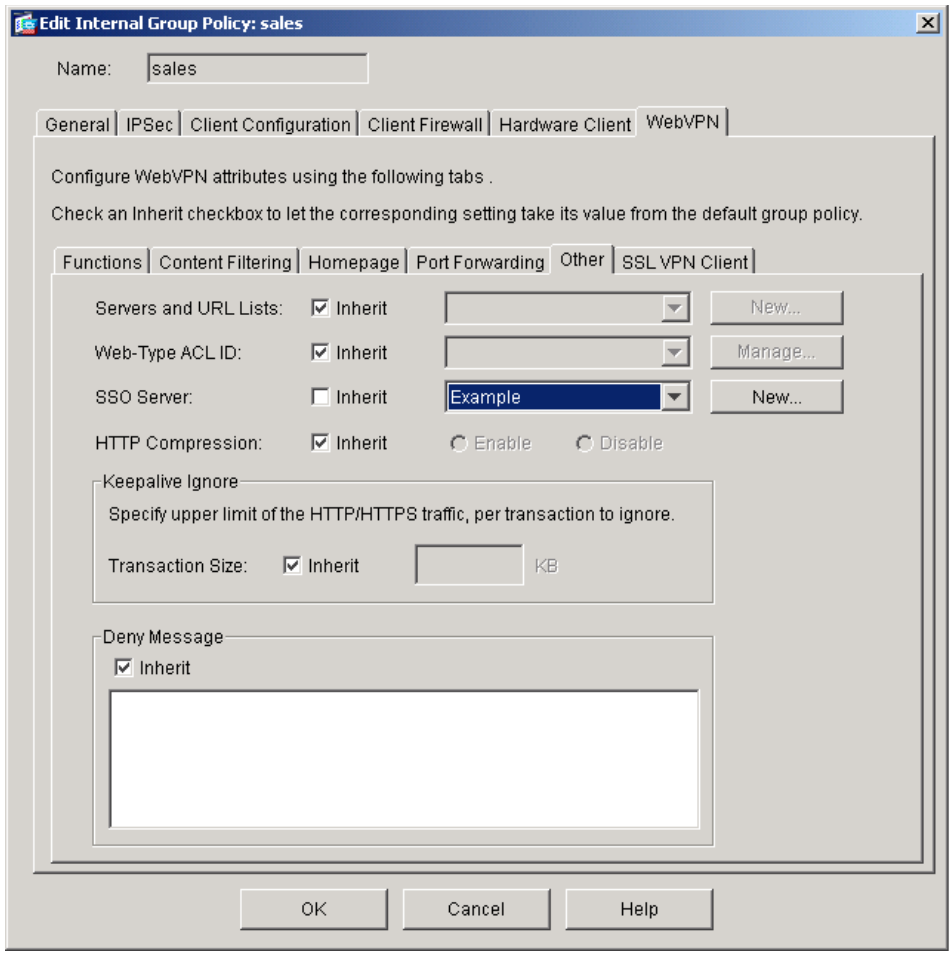


Step 2 In the Group Policy table, click the group policy to which you want to assign the SiteMinder SSO server.

Step 3 Click **Edit**.

The Edit Internal Group Policy dialog box appears as shown in Figure 8-5.

Figure 8-5 The Edit Internal Group Policy Dialog Box



Step 4 Click the **General** tab and then click the **Other** tab on the General tab.

Step 5 Next to SSO Server, do the following:

- Clear the SSO Server **Inherit** check box.
- Choose the new SSO server from the menu.

  In this example, the SSO server is named Example.

Step 6 Click **OK** to return to the ASDM window.

Step 7 Click **Apply** to enter the assignment into the running security appliance configuration.

Assigning the SSO Server to a User

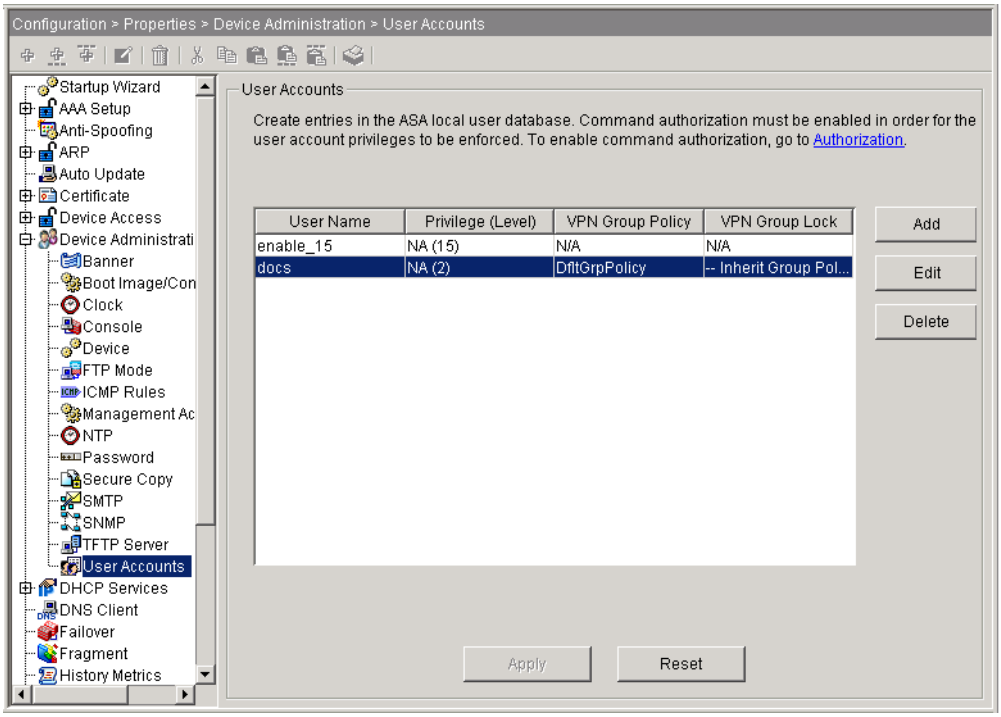
Note Comprehensive procedures for configuring users are provided elsewhere in this guide. The following steps are only those that apply to configuring a SiteMinder SSO server.

You can also assign the SSO server to a user by performing the following steps:

Step 1 In the main Cisco ASDM window, choose **Configuration > Properties > Device Administration > Users**.

The User Accounts area appears in the window as shown in Figure 8-6.

Figure 8-6 ASDM Window with User Accounts Area Displayed

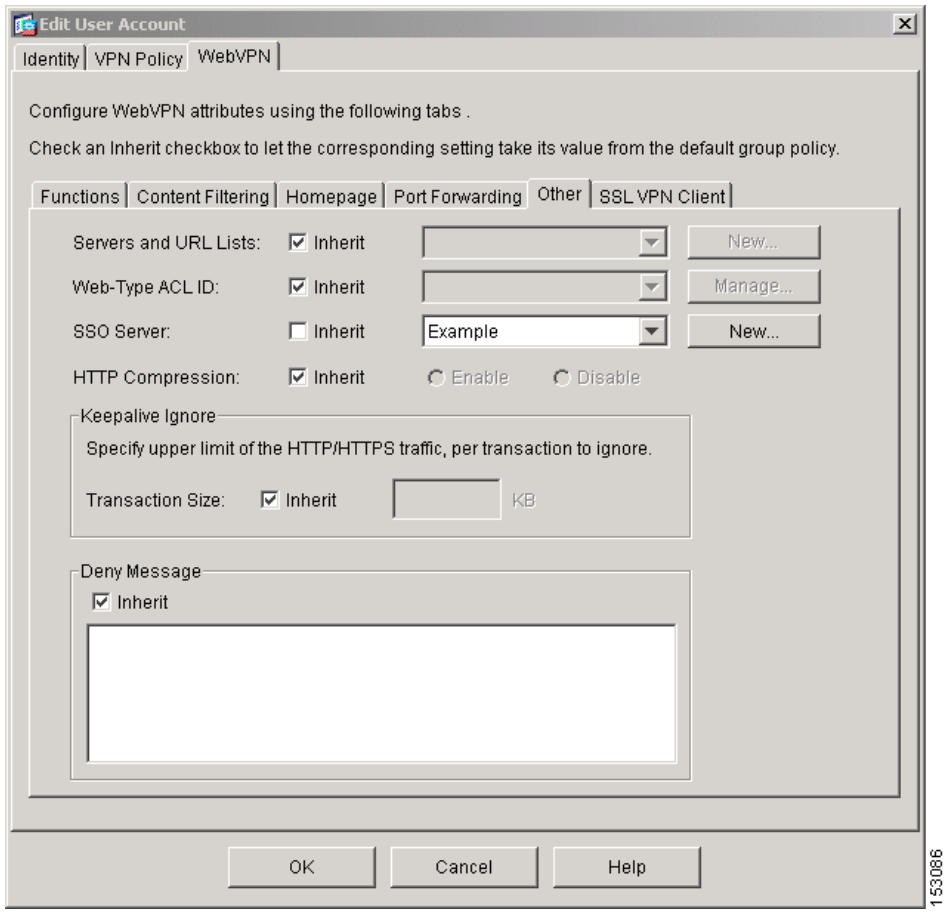


Step 2 From the User Accounts table, click the User Name you want to assign the SiteMinder SSO server to.

Step 3 Click **Add**.

The Edit User Account dialog box appears as shown in Figure 8-7.

Figure 8-7 The Edit User Account Dialog Box



Step 4 Click the **WebVPN** tab and then click the **Other** tab on the WebVPN tab.

Step 5 Next to SSO Server, do the following:

- Clear the SSO Server **Inherit** check box.
- Choose the new SSO server from the menu.

  In this example, the SSO server is named Example, as shown in Figure 8-7.

Step 6 Click **OK** to return to the ASDM window.

Step 7 Click **Apply** to enter the assignment into the running security appliance configuration.

Adding the Cisco Authentication Scheme to SiteMinder

Besides configuring the security appliance for SSO with SiteMinder, you must also configure your Computer Associates SiteMinder Policy Server with the Cisco authentication scheme, provided as a Java plug-in.

Note

- Configuring the SiteMinder Policy Server requires experience with SiteMinder.
- This section presents general tasks, not a complete procedure.
- Refer to the CA SiteMinder documentation for the complete procedure for adding a custom authentication scheme.

To configure the Cisco authentication scheme on your SiteMinder Policy Server, perform these following tasks:

Step 1 With the Siteminder Administration utility, create a custom authentication scheme being sure to use the following specific arguments:

- In the Library field, enter **smjavaapi**.
- In the Secret field, enter the same secret configured on the security appliance.

  You configure this on the security appliance with either the **policy-server-secret** command at the command line interface or in the Secret Key field of the Add SSO Server dialog box in ASDM.
- In the Parameter field, enter **CiscoAuthAPI**.

Step 2 Using your Cisco.com login, download the file **cisco_vpn_auth.jar** from http://www.cisco.com/cgi-bin/tablebuild.pl/asa and copy it to the default library directory for the SiteMinder server.

Configuring SSO with the HTTP Form Protocol

This section describes using the HTTP Form protocol for SSO. The HTTP Form protocol is a common approach to SSO authentication that can also qualify as a AAA method. It provides a secure method for exchanging authentication information between WebVPN users and authenticating web servers. As a common protocol, it is highly compatible with web servers and web-based SSO products, and you can use it in conjunction with other AAA servers such as RADIUS or LDAP servers.

As with SiteMinder, the security appliance serves as a proxy for WebVPN users to an authenticating web server but, in this case, it uses HTTP Form protocol and the POST method for requests. You must configure the security appliance to send and receive form data.

Note To configure SSO with the HTTP Form protocol correctly, you must have a thorough working knowledge of authentication and HTTP protocol exchanges.

While you would expect to configure form parameters that let the security appliance include POST data such as the username and password, you initially might not be aware of additional hidden parameters that the web server requires. Some authentication applications expect hidden data which is neither visible to nor entered by the user. You can, however, discover hidden parameters that the authenticating

web server expects by making a direct authentication request to the web server from your browser without the security appliance in the middle acting as a proxy. Analyzing the web server response using a HTTP header analyzer reveals hidden parameters in a format similar to the following:

```
<param name>=<URL encoded value>&<param name>=<URL encoded>
```

Some hidden parameters are mandatory and some are optional. If the web server requires data for a hidden parameter, it rejects any authentication POST request that omits that data. Because a header analyzer does not tell you if a hidden parameter is mandatory or not, we recommend that you include all hidden parameters until you determine which are mandatory.

This section describes:

- Gathering HTTP Form Data, page 8-10
- Configuring SSO with HTTP Form Protocol, page 8-13
- Assigning the SSO Server to a Tunnel Group, page 8-16

Gathering HTTP Form Data

This section presents the steps for discovering and gathering the HTTP Form data required to configure SSO if you do not already know what the data is. To gather the data, you must analyze responses from the authenticating web server using an HTTP header analyzer.

To gather parameter data, perform the following steps:

Step 1 Start your browser and HTTP header analyzer, and connect directly to the web server login page without going through the security appliance.

The web server login page loads into your browser.

Step 2 Examine the login exchange with your HTTP header analyzer. If the web server has loaded a cookie with the login page, copy this login page URL. It is the Start URL.

Step 3 Enter the username and password to log in to the web server, and press **Enter**.

This action generates the authentication POST request that you examine using the HTTP header analyzer.

An example POST request with host HTTP header and body follows:

```
POST
/emco/myemco/authc/forms/MCOlogin.fcc?TYPE=33554433&REALMOID=06-000430e1-7443-125c-ac05-83
846dc90034&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=$SM$5FZmjnk3DRNwNjk2KcqVCFbIrNT9%2b
J0H0KPshFtg6rB1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F%2Fwww.example.com%2Femco%2Fmyemco%2F
HTTP/1.1
Host: www.example.com
(BODY)
SMENC=ISO-8859-1&SMLOCALE=US-EN&USERID=Anyuser&USER_PASSWORD=XXXXXX&target=https%3A%2F%2Fw
ww.example.com%2Femco%2Fmyemco%2F&smauthreason=0
```

Step 4 Examine the POST request and copy the protocol, host, and the complete URL. This is needed to configure the action-uri parameter later.

Step 5 Examine the POST request body and copy the following:

a. Username parameter

In this example, the parameter is userid (not the value anyuser).

b. Password parameter

In this example, the parameter is user_password.

c. Hidden parameter

This parameter is everything in the POST body except the username and password parameters. In this example, the hidden parameter is:
SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Fwww.example.com%2Femco%2Fmyemco%2F&smauthreason=0

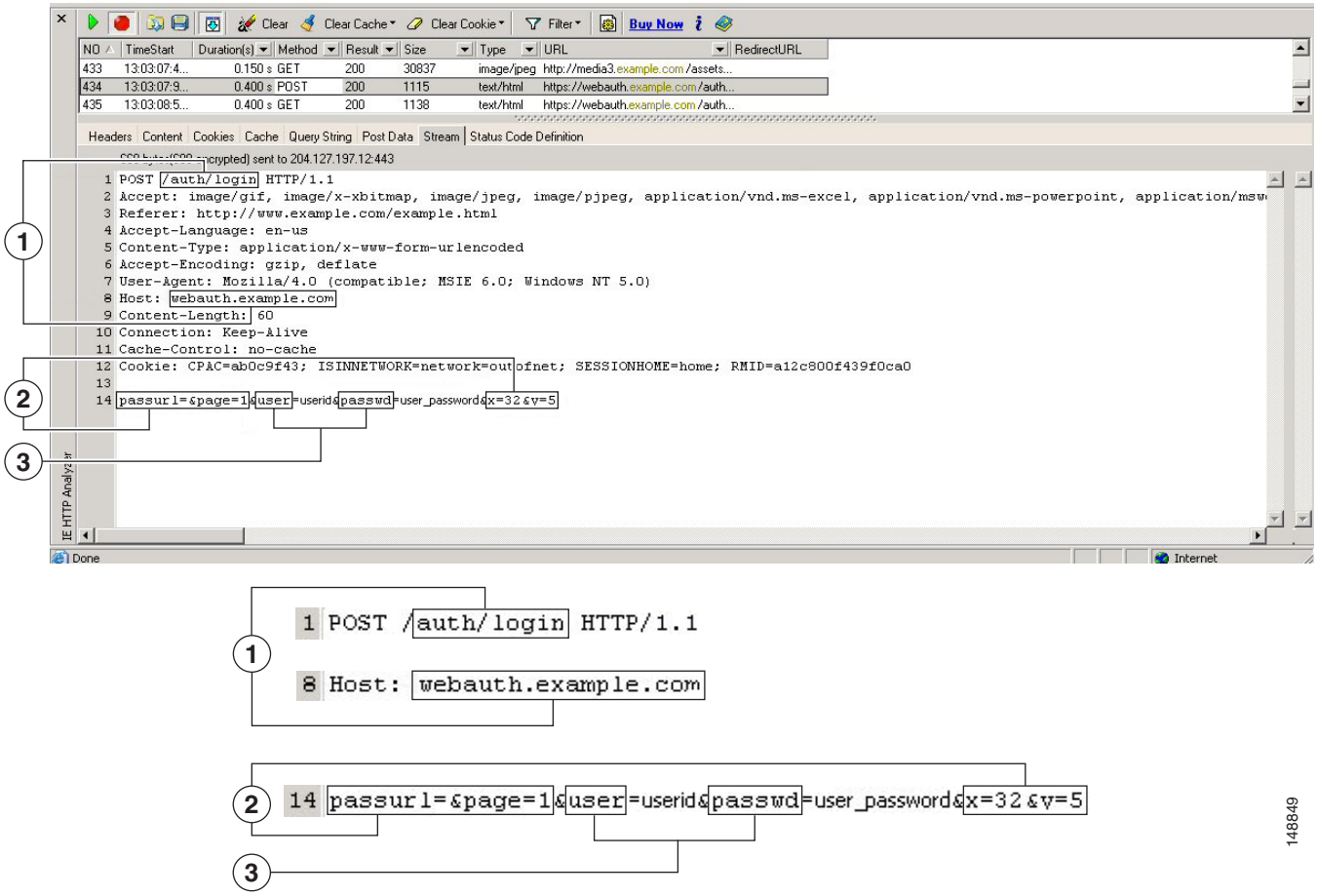
Hidden parameters are typically presented in the following format:

<param name>=<URL encoded value>&<param name>=<URL encoded>

Some hidden parameters are mandatory and some are optional. If the web server requires data for a hidden parameter, it rejects any authentication POST request that omits that data. Because a header analyzer does not tell you if a hidden parameter is mandatory or not, we recommend that you include all hidden parameters until you determine which are mandatory.

Figure 8-8 highlights the action URI, hidden, username and password parameters found using an HTTP header analyzer. This is only an example; output varies widely across different websites.

Figure 8-8 Action-uri, hidden, username and password parameters



1	Action URI parameter
2	Hidden parameters
3	Username and password parameters

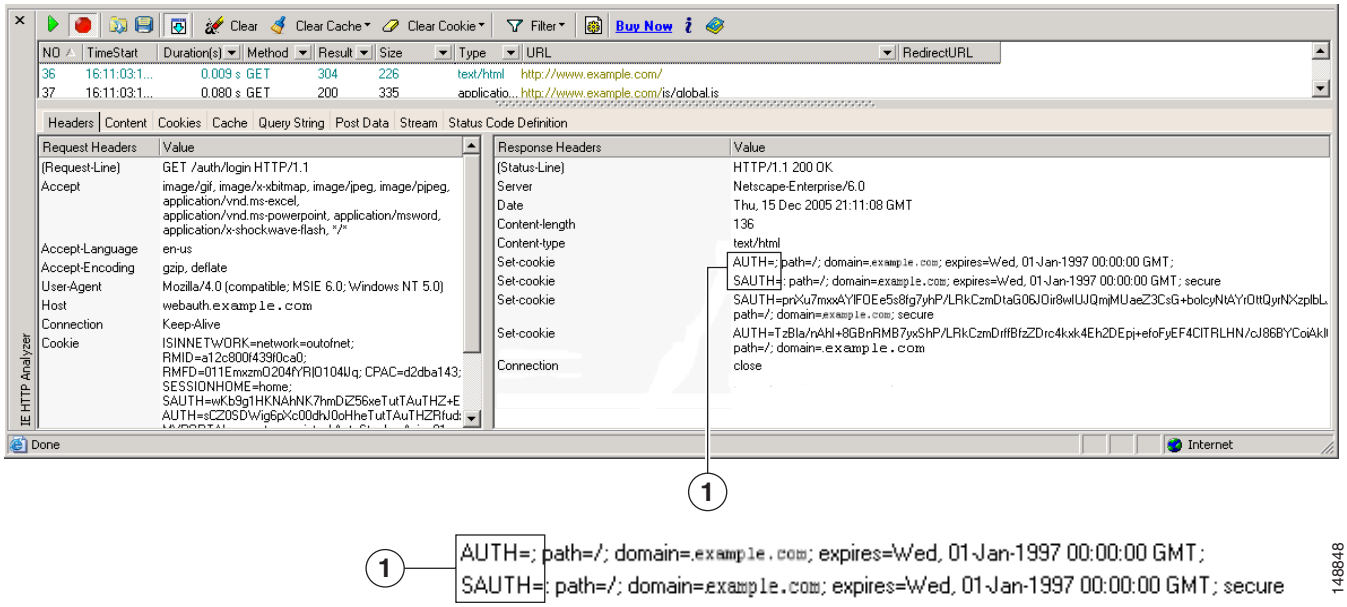
Step 6 If you successfully log in to the web server, examine the server response with the HTTP header analyzer to locate the name of the session cookie set by the server in your browser. This is the Authentication Cookie Name value.

In the following server response header, the name of the session cookie is SMSESSION. You just need the name, not the value.

```
Set-Cookie:
SMSESSION=yN4Yp5hHVNDgs4FT8dn7+Rwev41hsE49XlKc+1twie0gqnjbhkTkUnR8XWP3hvDH6PZPbHIHtWLDKTa8
ngDB/lbYTjIxrbDx8WPWwaG3CxVa3adOxHFR8yjD55GevK3ZF4ujgU1lhO6fta0dSSOSepWvnsCb7IFxCw+MGiw0o8
8uHa2t4l+SillqfJvcpuXfiIAO06D/gtDF40Ow5YKHEl2KhDEvv+yQzxwfEz2cl7Ef5iMr8LgGcDK7qvMcvrgUqx68
JQOK2+RSwtHQ15bCZmsDU5vQVCvSQWC8OMHNGwpS253XwRLvd/h6S/tM0k98QMv+i3N8oOdj1V7flBqecH7+kVrU01
F6oFzr0zM1kMyLr5HhlVDh7B0k9wp0dUFZiAzaf43jupD5f6CEkuLeudYW1xgNzsR8eqtPK6t1gFJyOn0s7QdNQ7q9
ZL2RwmP9JV5l48I3XBFPNUw/3V5jf7nRuLr/CdfK3OO8+Pa3V6/nNhokErSgyxjzMd88DVzM41LxxaUDhbcmkoHT9I
mzBvKzJX0J+o7FoUDFOxEdIqlAN4GNqk49cpi2sXDbIarALp6Bl3+tbB4MlHGH+0CPscZXqoi/kon9YmGauHyRs+0m
6wthdlAmCnvlJCDfDoXtn8DpabgiW6VDTrvl3SGPyQtUv7Wdahuq5SxbUzjY2JxQnrUtwB977NCzYu2sOtN+dsEReW
J6ueyJBbMzKyzUB4L3i5uSYN50B4PCv1w5KdRKa5p3N0Nfq6RM6dfipMEJw0Ny1sZ7ohz3fbvQ/YZ7lw/k7ods/8Vb
aR15ivkE8dSCzuf/AInHtCzuQ6wApzEp9CUoG8/dapWriHjNoi4llJOgCst33wEhxFxcWy2UWxs4EZSjsI5GyBnefS
QTPVfma5dc/emWor9vWr0HnTQaHP5rg5dTNqunkDEdMIHfbeP3F90cZejVzihM6igiS6P/CEJAjE;Domain=.examp
le.com;Path=/
```

Figure 8-9 shows an example of authentication cookies in HTTP analyzer output. This is only an example; output varies widely across different websites.

Figure 8-9 Authentication cookies in sample HTTP analyzer output



1	Authentication cookies

In some cases, the server may set the same cookie regardless of whether the authentication was successful or not. Such a cookie is unacceptable for SSO purposes.

Step 7 To confirm that the cookies are different, repeat Step 1 through Step 6 using invalid login credentials and then compare the “failure” cookie with the “success” cookie. You now have the necessary parameter data to configure the security appliance for SSO with HTTP Form protocol.

Configuring SSO with HTTP Form Protocol

This section presents an example procedure for configuring SSO with the HTTP Form protocol using the parameters gathered in the previous section. In this procedure, there are steps that are always required and steps that are sometimes required. The steps that are always required are the configuration of the:

- Action URI
- Username parameter
- Password parameter

The other steps are only required if the authenticating web server requires them. They are the configuration of:

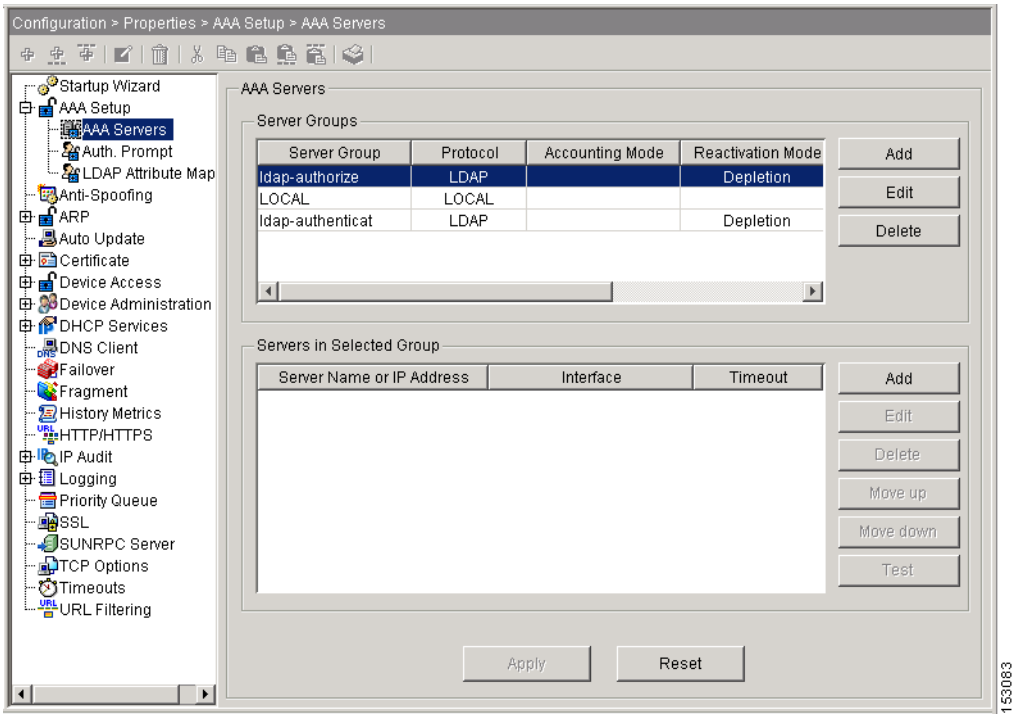
- A start URL
- Hidden parameters
- An authentication cookie name

Perform the following steps to configure the security appliance to use HTTP Form protocol for SSO:

Step 1 In the main Cisco ASDM window, choose **Configuration > Properties > AAA Setup > AAA Servers**.

The AAA Servers area appears in the window as shown in Figure 8-10.

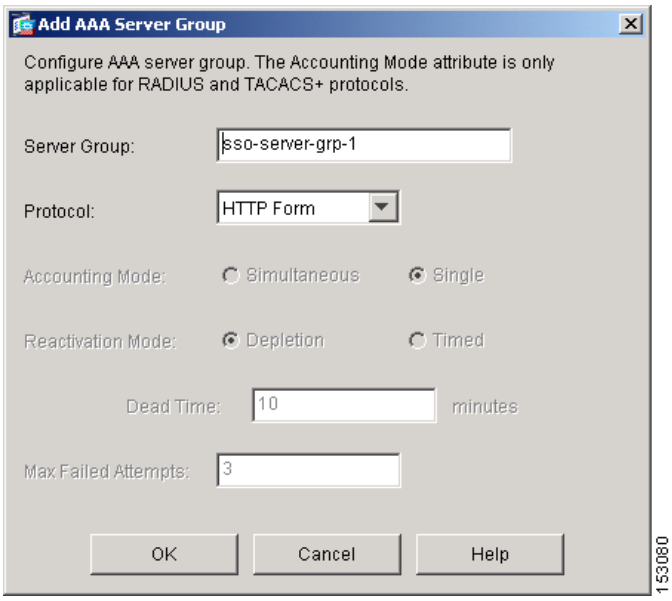
Figure 8-10 ASDM Window with AAA Servers Area Displayed



Step 2 Click **Add** in the Server Groups area.

The Add AAA Server Group dialog box appears as shown in Figure 8-11.

Figure 8-11 The Add AAA Server Group Dialog Box



Step 3 Enter the name of the server group in the Server Group field.

In this example, the name of the server group is sso-server-grp-1.

Step 4 From the Protocol menu, choose **HTTP Form**.

The remaining dialog box elements become unavailable.

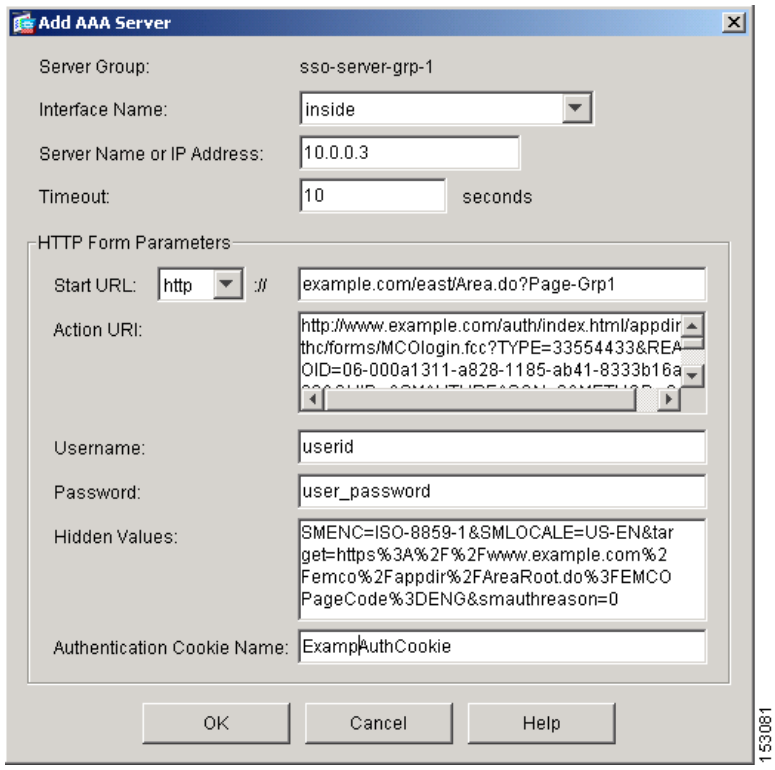
Step 5 Click **OK** to return to the ASDM window.

Step 6 If it is not already selected, click on the server group you just created to select it.

Step 7 Click **Add** in the Servers in Selected Group area.

The Add AAA Server dialog box appears. Figure 8-12 shows this dialog box completed with the values described in Step 8 through Step 16.

Figure 8-12 The Add AAA Server Dialog Box



Step 8 From the Interface Name menu, choose **inside**, **outside**, or **management**.

In this example, we choose **inside**. Interface name selection does not effect functionality.

Step 9 In the Server Name or IP Address field, enter either the name or address of the authenticating web server.

In this example, we enter the internal IP address.

Step 10 In the Timeout field, enter the time in seconds before a failed SSO authentication attempt times out.

Step 11 If the authenticating web server sets a pre-login cookie, configure the start URL from which to retrieve the pre-login cookie from the web server by performing the following steps:

a. In the Start URL menu, choose one of the following:

- **http** for unencrypted messaging between the security appliance and the web server

  -or-

- **https** for secure messaging between the security appliance and the web server

b. In the Start URL field, enter the rest of the complete start URL for the authenticating web server.

In this example, the complete start URL is http://example.com/east/Area.do?Page-Grp1.

Step 12 In the Action URI field, enter the URI for the authentication program on the web server.

The maximum number of characters for a complete URI is 2048. The action URI in this example follows:

```
http://www.example.com/auth/index.html/appdir/authc/forms/MCOlogin.fcc?TYPE=33554433&REALM
OID=06-000a1311-a828-1185-ab41-8333b16a0008&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=$S
M$5FZmjnk3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6rB1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F%2Fauth
.example.com
```

Note You must include the hostname and protocol in the action URI. In the preceding example, these appear at the start of the URI in http://www.example.com.

Step 13 In the Username field, enter the name of the username parameter for the HTTP POST request.

In this example, the username parameter is named userid.

Step 14 In the Password field, enter the name of the password parameter for the HTTP POST request.

In this example, the password parameter is named user_password.

Step 15 If the web server expects hidden parameters in the POST request, enter the hidden parameters expected in the Hidden Values field.

In this example, the Hidden Values entry is:

SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Fwww.example.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG&smauthreason=0

This entry, excerpted from a POST request, includes four form entries and their values, each separated by an &. The four entries and their values are:

- SMENC with a value of ISO-8859-1
- SMLOCALE with a value of US-EN
- target with a value of https%3A%2F%2Fwww.example.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG
- smauthreason with a value of 0

Step 16 Enter the name of the authentication cookie in the Authentication Cookie Name field. This step is optional.

In this example, the authentication cookie name is ExampAuthCookie.

Step 17 Click **OK** to return to the ASDM window.

Step 18 Click **Apply** to add the new SSO server and server group to the running configuration.

Assigning the SSO Server to a Tunnel Group

The final task is to assign the new SSO server to a new or existing tunnel group. In this example, we assign the SSO server to a new WebVPN tunnel group named WebVPNGroup1 by performing the following steps:

Step 1 In the main Cisco ASDM window, choose **Configuration > VPN > General > Tunnel Group**.

Step 2 Click **Add** and choose **WebVPN Access**.

The Add Tunnel Group dialog box appears with the General and Basic tabs displayed.

Step 3 Enter the name of the new tunnel group in the Name field.

In this example, the name is WebVPNGroup1.

Step 4 Click the **AAA** tab and select the new SSO server group from the Authentication Server Group menu.

In this example, the name of the server group is sso-server-grp-1.

Step 5 Click **OK** to return to the **Configuration > VPN > General > Tunnel Group** window, and then click **Apply** to add the tunnel group to the running configuration.

Configuring Network Admission Control

This chapter includes the following sections.

Uses, Requirements, and Limitations

Network Admission Control (NAC) protects the enterprise network from intrusion and infection from worms, viruses, and rogue applications by performing endpoint compliancy and vulnerability checks as a condition for production access to the network. We refer to these checks as *posture validation.* You can configure posture validation to ensure that the anti-virus files, personal firewall rules, or intrusion protection software on a host establishing an IPSec session are up-to-date. Posture validation can include the verification that the applications running on the remote hosts are updated with the latest patches. NAC supplements the identity-based validation that IPSec and other access methods provide. It is especially useful for protecting the enterprise network from hosts that are not subject to automatic network policy enforcement, such as home PCs.

Note When configured to support NAC, the security appliance functions as a client of a Cisco Secure Access Control Server, requiring that you install a minimum of one Access Control Server on the network to provide NAC authentication services. ASA support for NAC is limited to remote access IPSec and L2TP over IPSec sessions. NAC on the ASA does not support WebVPN, non-VPN traffic, IPv6, and multimode.

Configuring a Connection to an Access Control Server

The instructions in the following sections assume you have added at least one Access Control Server to the network to support NAC:

Configuring the Access Control Server Group

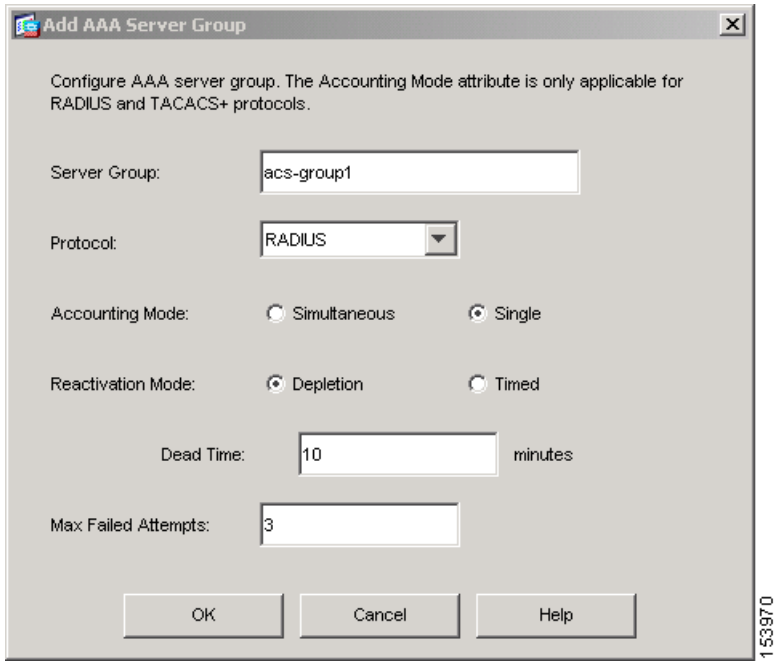
You must configure an Access Control Server group even if the network has only one Access Control Server.

Configure an Access Control Server group, as follows:

Step 1 Choose Configuration > Properties > AAA Setup > AAA Server Groups, then click **Add** to the right of the AAA Server Groups table.

The AAA Server Groups window opens (Figure 9-1).

Figure 9-1 Add AAA Server Group Window



Step 2 See the following descriptions to assign values to the attributes in this window.

- **Server Group**—Enter a name for the server group.

Note If a RADIUS server is configured to return the Class attribute (#25), the security appliance uses that attribute to authenticate the Group Name. On a RADIUS server, the attribute must be in the format OU=*groupname*, where *groupname* is identical to the Server Group name on the security appliance.

- **Protocol**—Indicates whether this is a RADIUS or an LDAP server group. Select **RADIUS** for an Access Control Server group.
- **Accounting Mode**—(*RADIUS and TACACS+ protocols only*) Click **Simultaneous** to configure the security appliance to send accounting data to all servers in the group, or click **Single** to send accounting data to only one server.

- **Reactivation Mode**—Click **Depletion** to reactivate connections to failed servers only after all of the servers in the group become inactive, or click **Timed** to reactivate them after 30 seconds of downtime.
- **Dead Time**—(for Depletion mode only) Enter the number of minutes that must elapse between the disabling of the last server in the group and the subsequent re-enabling of all servers.
- **Max Failed Attempts**— Enter an integer in the range 1 through 5 to configure the number of failed connection attempts the security appliance allows before declaring a nonresponsive server inactive.

Step 3 Click **OK**.

ASDM displays the group you added in the AAA server groups table in the Configuration > Properties >AAA Setup > AAA Server Groups table.

Use the next section to add the server to the group.

Adding an ACS to the ACS Group

Add one or more Access Control Servers to an ACS group as follows:

Step 1 Choose Configuration > Properties > AAA Setup > AAA Server Groups.

The AAA Server Groups table lists the groups configured on this security appliance.

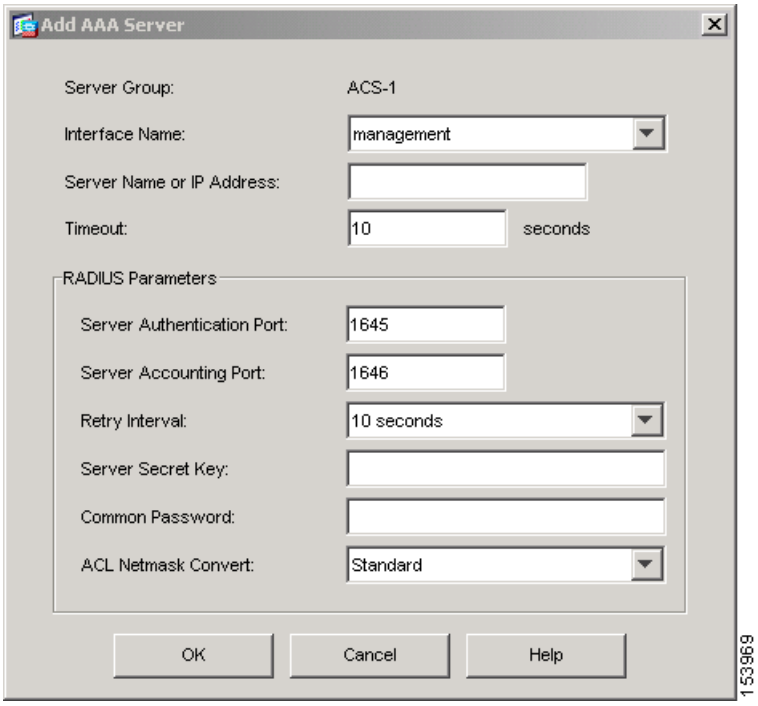
Step 2 Select the ACS group you created in the previous section.

ASDM highlights the group and displays the contents of the group in the Servers in the selected group table.

Step 3 Click **Add** to the right of the Servers in the selected group table.

The Add AAA Server window opens (Figure 9-2).

Figure 9-2 Add AAA Server Window



Step 4 Assign values to the attributes in this window consistent with those configured on the ACS. The attribute descriptions are as follows:

- **Server Group**—*Display only.* Shows the name of the server group to which you are the ACS server.
- **Interface Name**—Select the network interface through which the security appliance connects to the server.
- **Server Name or IP Address**—Enter a name or the IP address of the AAA server.
- **Timeout**—Enter the timeout interval, in seconds. The security appliance gives up on the request to the primary AAA server after this timer expires. If a standby AAA server is present in the configuration and the connection to the primary server times out, the security appliance sends the request to the backup server.
- **Server Authentication Port**—Enter the number of the server port for user authentication. The default port is 1645.

Note The latest RFC states that RADIUS should be on UDP port number 1812, so you might need to change this default value to 1812.

- **Server Accounting Port**—Enter the server port to use for user accounting. The default port is 1646.
- **Retry Interval**—Enter the number of seconds before reattempting a connection after sending a query to the server and receiving no response. Enter the number of seconds in the range 1 through 10. The default value is 10 seconds.

- **Server Secret Key**—Enter the server secret key (also called the shared secret) to use for encryption; for example, C8z077f. The secret is case-sensitive. The field displays only asterisks. The security appliance uses the server secret to authenticate to the Access Control Server. The server secret you configure here should match the one configured on the Access Control Server. The maximum field length is 64 characters.
- **Common Password**—Enter the common password for the group. The password is case-sensitive. The field displays only asterisks. If you are defining a RADIUS server to be used for authentication rather than authorization, do not provide a common password.

  A RADIUS authorization server requires a password and username for each connecting user. You enter the password here. The RADIUS authorization server administrator must configure the RADIUS server to associate this password with each user via this security appliance. Be sure to provide this information to your RADIUS server administrator. Enter a common password for all users who are accessing this RADIUS authorization server through this security appliance.

  If you leave this field blank, each user password will be the username. As a security precaution never use a RADIUS authorization server for authentication. Using common passwords or usernames as passwords is much less secure than using a strong password for each user.

Note The password field is required by the RADIUS protocol and the RADIUS server requires it; however, users do not need to know it.

- **ACL Netmask Convert**—Select the method by which the security appliance handles netmasks received in downloadable access lists. The security appliance expects downloadable access lists to contain standard netmask expressions. A wildcard mask has ones in bit positions to ignore and zeroes in bit positions to match. The ACL Netmask Convert list helps minimize the effects of these differences on how you configure downloadable access lists on your RADIUS servers.

  If you choose **Detect Automatically**, the security appliance attempts to determine the type of netmask expression used. If it detects a wildcard netmask expression, it converts it to a standard netmask expression; however, because some wildcard expressions are difficult to detect unambiguously, this setting may occasionally misinterpret a wildcard netmask expression as a standard netmask expression.

  If you choose **Standard**, the security appliance assumes downloadable access lists received from the RADIUS server contain only standard netmask expressions. The security appliance does not translate wildcard netmask expressions.

  If you choose **Wildcard**, the security appliance assumes downloadable access lists received from the RADIUS server contain only wildcard netmask expressions, and it converts them all to standard netmask expressions when the access lists are downloaded.

Step 5 Click **OK**.

ASDM displays the server you added in the Servers in selected group table.

Now that you have added the ACS server to the server group, use the instructions in the next section to assign the server group to the group policy.

Assigning the ACS Server Group as the NAC Authentication Server

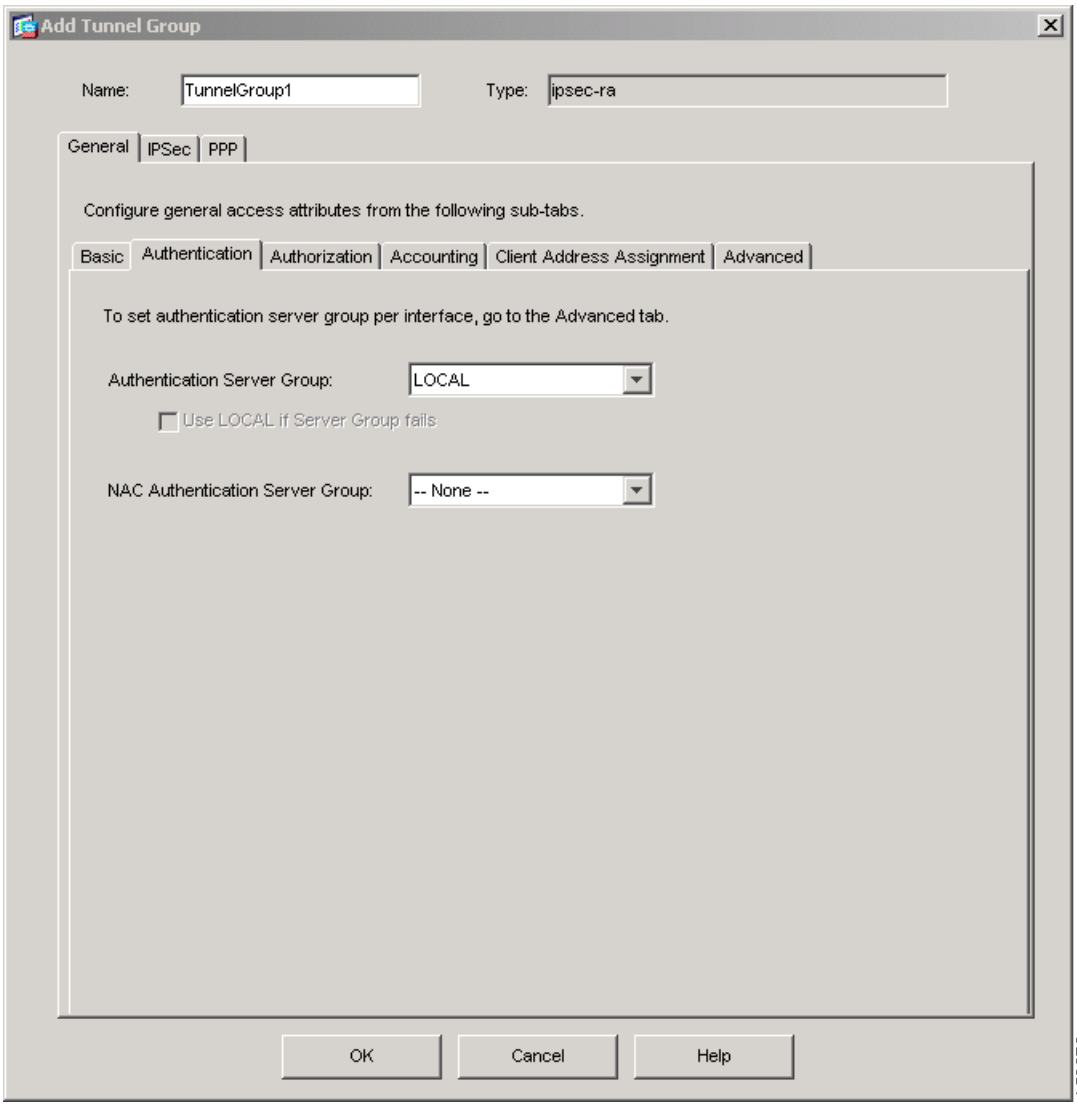
Add the ACS Server Group as the NAC Authentication Server for the default tunnel group, or to alternative tunnel groups for which you want to configure support for NAC, as follows:

Step 1 Choose Configuration > VPN > General > Tunnel Group.

Step 2 Double-click the tunnel group named DefaultRAGroup or an alternative tunnel group configured for remote access (Type is "ipsec-ra") on which you want to configure NAC support, or click **Add > IPSec for Remote Access** to add a new tunnel group.

Step 3 Click the General tab > Authentication tab. (Figure 9-3).

Figure 9-3 General Tab > Authentication Tab



Step 4 Set the attributes in this window, as follows:

- **Authentication Server Group**—Lists the available authentication server groups, including the LOCAL group (the default setting). You can select None. Selecting an option other than None or Local makes available the Use LOCAL if Server Group Fails check box. (The Advanced tab lets you assign an authentication server group to each interface.)
- **Use LOCAL if Server Group fails**—Check this attribute to enable fallback to the LOCAL database if the group specified by the Authentication Server Group attribute fails. Uncheck to disable fallback.
- **NAC Authentication Server Group**—Select an ACS group consisting of at least one server configured to support NAC. The list displays the names of all server groups of type RADIUS configured on this security appliance that are available for remote access tunnels.

Step 5 Click **OK**.

Enabling NAC and Assigning NAC Properties to a Group Policy

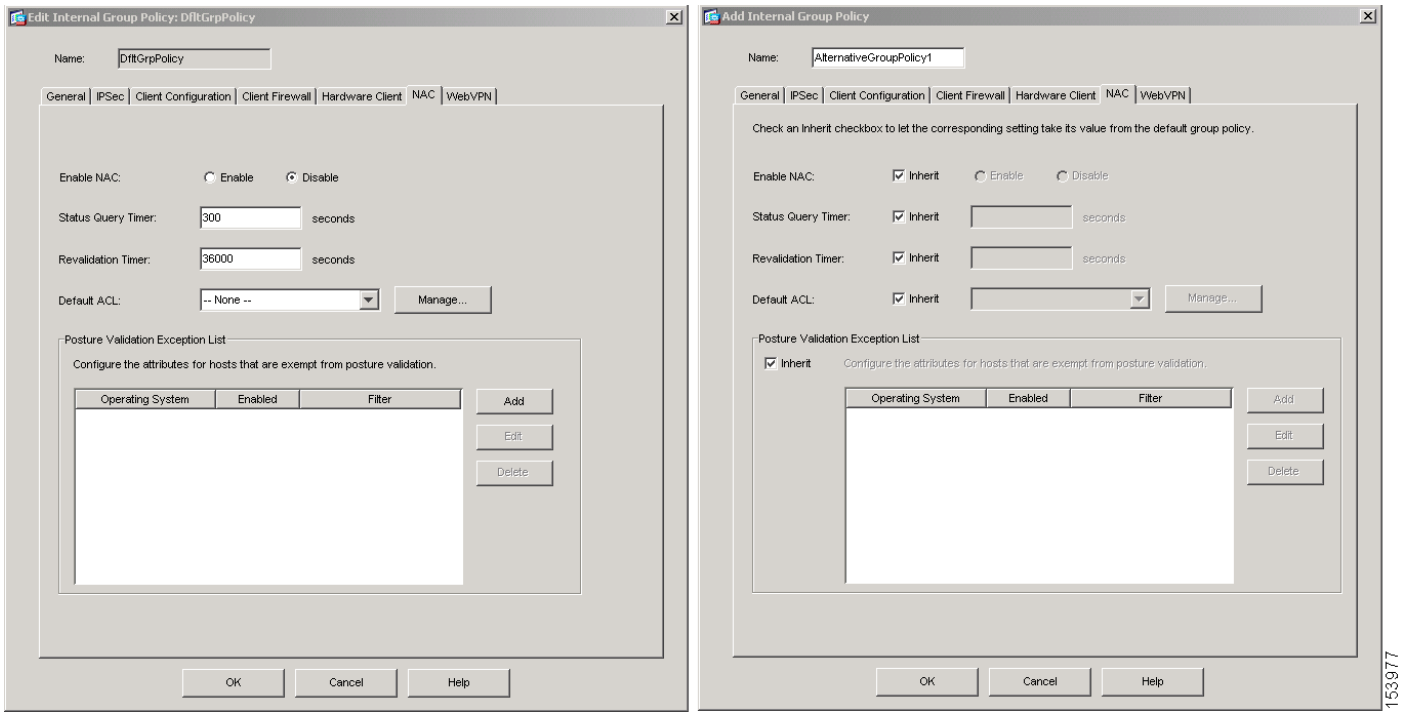
Enable NAC on the default group policy or on alternative IPSec group policies, and view or modify its default settings, as follows:

Step 1 Choose Configuration > VPN > General > Group Policy.

Step 2 Double-click the policy named DfltGrpPolicy or an alternative group policy configured for remote access (Tunneling Protocol is “IPSec”) for which you want to enable NAC, or click **Add** > **Internal Group Policy** to add a new group policy.

Step 3 Open the NAC tab (Figure 9-4).

Figure 9-4 NAC Tab on the DfltGrpPolicy and an Alternative Group Policy



Note If you check the Inherit check box in an alternative group policy, the policy uses the setting on the default group policy. Clearing the Inherit check box allows you to customize an alternative group policy setting, making it independent from the default group policy setting.

Step 4 Set the attributes in this window, as follows:

- **Enable NAC**—Click **Enable** to execute Network Admission Control procedures to validate eligible hosts associated with this group policy and assign them the ACL downloaded from the Access Control Server if they pass posture validation checks, or click **Disable** to not perform NAC procedures.

  Note The remaining attributes are effective only if NAC is enabled.

- **Status Query Timer**—After each successful posture validation, the security appliance starts a status query timer. The expiration of this timer triggers a query to the remote host for changes in posture since the last posture validation. A response indicating no change resets the status query timer. A response indicating a change in posture triggers an unconditional posture revalidation. The security appliance maintains the current access policy during revalidation.

  By default, the interval between each successful posture validation and the status query, and each subsequent status query, is 300 seconds (5 minutes). The group policy inherits the value of the status query timer from the default group policy unless you change it. To do so, enter a number in the range 300 to 1800 seconds (5 to 30 minutes).

- **Revalidation Timer**—After each successful posture validation, the security appliance starts a revalidation timer. The expiration of this timer triggers the next unconditional posture validation. The security appliance maintains the current access policy during revalidation. By default, the

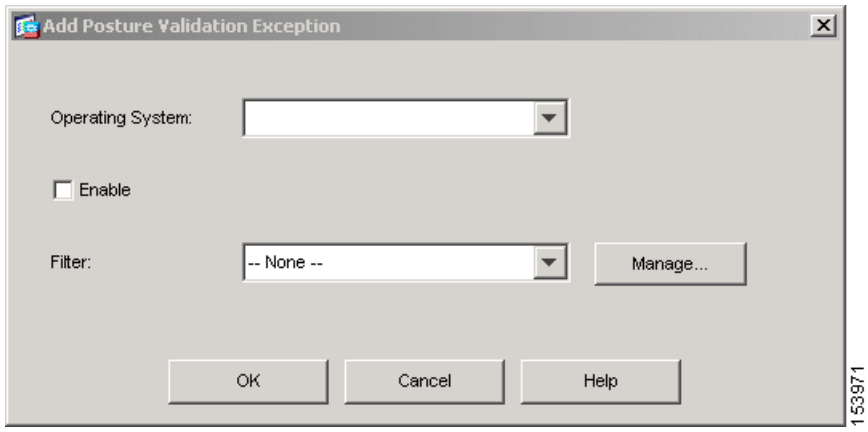
interval between each successful posture validation is 36000 seconds (10 hours). The group policy inherits the value of the revalidation timer from the default group policy unless you change it. To do so, enter a number in the range 300 to 86400 seconds (5 minutes to 24 hours).

- **Default ACL**—The security appliance applies the ACL identified by this attribute to hosts that are eligible for NAC, before posture validation. Following posture validation, the security appliance replaces the default ACL with the one obtained from the Access Control Server for the remote host. It applies this ACL if revalidation fails. if clientless authentication is enabled, the security appliance also applies this ACL to hosts that do not have a Cisco Trust Agent to respond to posture validation requests. Select the ACL to use as the default ACL for NAC sessions, or use the default setting, **None**, to not apply a default ACL.

  To add an ACL to the drop-down list, view the configuration of the ACLs in the list, or modify an ACL in the list, click **Manage**. The ACL Manager window opens. For instructions, see "Managing ACLs and ACEs" on page 2-13.

- **Posture Validation Exception List**—A Yes value in the Enabled column indicates that the associated operating system is exempt from posture validation. A No value indicates that the exemption entry is present in the configuration, but that the security appliance ignores it. The Filter is optional. In addition to exempting the computer from posture validation, the security appliance applies the ACL identified in the Filter column to filter the traffic if the computer's operating system matches and the Enabled value is Yes. To add or modify an entry in the list, click **Add**, or double-click the entry to be modified. The Add or Edit Posture Validation window opens (Figure 9-5).

Figure 9-5 Add Posture Validation Exception



Step 5 (Applies only if you are modifying the Posture Validation Exception List.) Set the attributes in the window, as follows:

- **Operating System**—Select the operating system running on the remote computer that you want to exempt from posture validation, or enter its name. For example, enter **Windows XP**.
- **Enable**—Check to enable the exemption. The default setting is unchecked, which disables the entry in the exemption list without removing it from the list.
- **Filter** to apply an ACL to filter the traffic if the operating system running on the computer matches the value of the Operating System attribute. Use the default option, **None**, if you do not want to apply a filter. Otherwise, select an ACL from the drop-down list.

To add an ACL to the drop-down list, view the configuration of the ACLs in the list, or modify an ACL in the list, click **Manage**. The ACL Manager window opens. For instructions, see "Managing ACLs and ACEs" on page 2-13.

Click **OK** after setting the attributes in the Add or Edit Posture Validation window. The NAC tab displays the new or modified entry in the Posture Validation Exception List.

Step 6 Click **OK**, then **Apply** to save the changes to the running configuration.

Changing Global NAC Settings

The security appliance provides default settings that apply to all NAC sessions. Use the instructions in this section to adjust these settings for adherence to the policies in force in your network.

The ASA provides default settings for the attributes that specify communications between the security appliance and the remote host. These attributes determine the maximum values of the expiration counters that impose limits on the communications with the Cisco Trust Agent on the remote host, and specify the port no. to communicate with the Cisco Trust Agent.

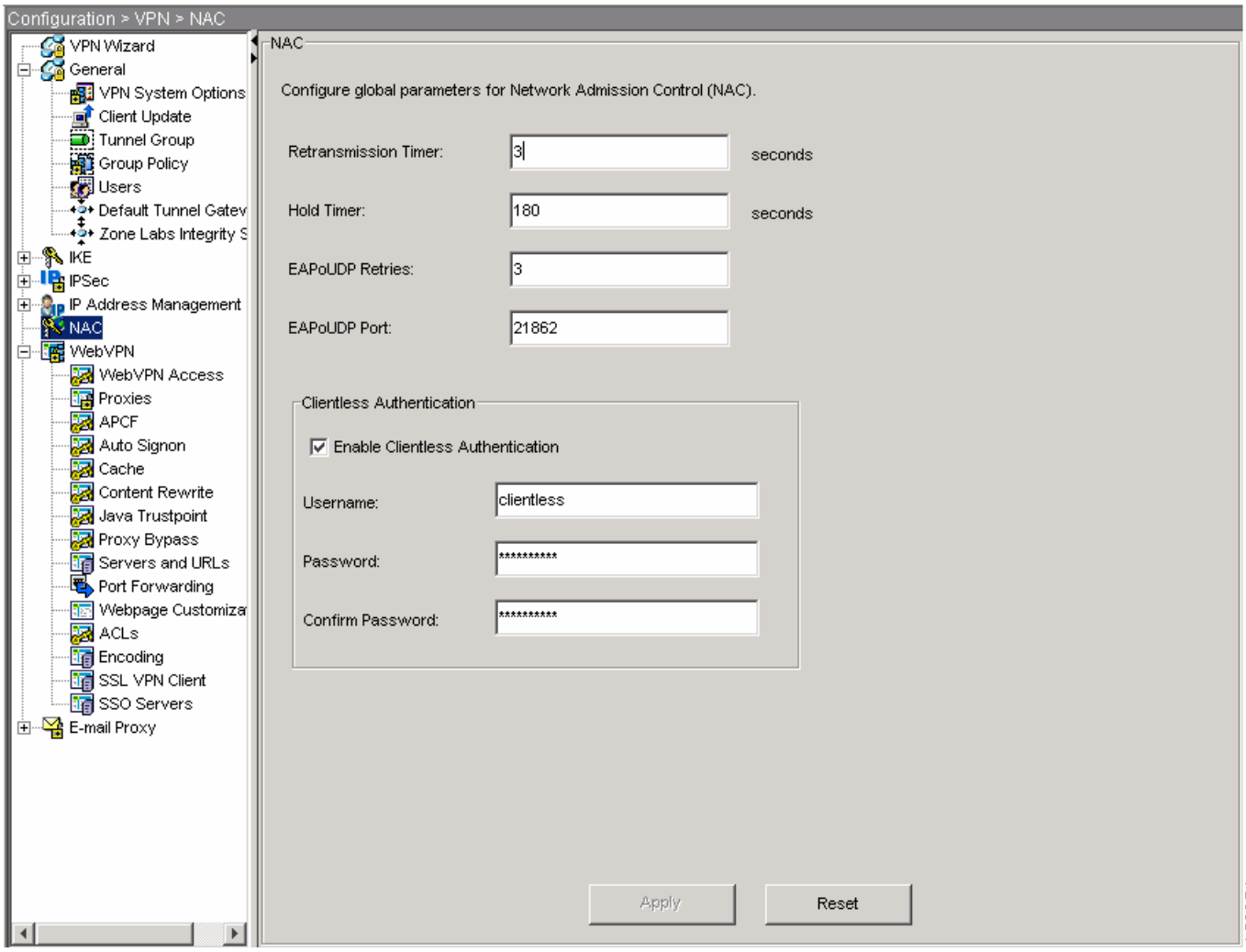
The global NAC settings also let you enable or disable clientless authentication, which applies a policy to hosts that do not have a Cisco Trust Agent to respond to posture validation requests.

View or modify the global NAC settings, as follows:

Step 1 Choose Configuration > VPN > NAC.

Step 2 ASDM opens the NAC window (Figure 9-6).

Figure 9-6 NAC



Note The attributes in this window are effective only if NAC is enabled on a group policy that the security appliance applies to an IPSec session.

Step 3 Set the attributes in this window, as follows:

- **Retransmission Timer**—When the security appliance sends an EAP over UDP request for a posture validation to a remote host, it waits for a response. If it fails to receive a response within the number of seconds assigned to this attribute, it resends the EAP over UDP message. By default, the retransmission timer is 3 seconds. Enter a value in the range 1 to 60 to change the duration of the wait period.
- **Hold Timer**—If the EAPoUDP Retries counter matches the EAPoUDP Retries value, the security appliance terminates the EAP over UDP session with the remote host and starts this timer. If this attribute equals *n* seconds, the security appliance establishes a new EAP over UDP session with the remote host. By default, the maximum number of seconds to wait before establishing a new session is 180 seconds. Enter the number of seconds in the range 60 to 86400 (24 hours) to change it.

- **EAPoUDP Retries**—When the security appliance sends an EAP over UDP message to the remote host, it waits for a response. If it fails to receive a response, it resends the EAP over UDP message. By default, it retries up to 3 times. Enter a value in the range 1 to 3 to change it.
- **EAPoUDP Port**—Enter the port no. on the client endpoint to be used for EAP over UDP communication with the Cisco Trust Agent. The default port no. is 21862. Enter a value in the range 1024 to 65535 to change it.
- **Enable Clientless Authentication**—Check to apply a policy to hosts that do not have a Cisco Trust Agent to respond to posture validation requests.

  When a host attempts to establish an IPSec session, the security appliance applies the default access policy, sends the EAP over UDP request for posture validation, and the request times out. If the security appliance is not configured to request a policy for clientless hosts from the Access Control Server, it retains the default access policy already in use for the clientless host.

  If clientless authentication is enabled, and the security appliance fails to receive a response to a validation request from the remote host, it sends a clientless authentication request on behalf of the remote host to the Access Control Server. The request includes the login credentials that match those configured for clientless authentication on the Access Control Server. The Access Control Server then provides the access policy to be enforced by the security appliance.

Note The remaining attributes apply only if you check **Enable Clientless Authentication**.

- **Username**—Enter the username configured on the Access Control Server to support clientless hosts. The default username is “clientless”. If you change it on the Access Control Server, you must also do so on the security appliance. You can enter 1 to 64 ASCII characters, excluding leading and trailing spaces, pound signs (#), question marks (?), quotation marks ("), asterisks (*), and angle brackets (< and >).
- **Password**—Enter the password configured on the Access Control Server to support clientless hosts. The default password is “clientless”. If you change it on the Access Control Server, you must also do so on the security appliance. You can enter 4 – 32 ASCII characters.
- **Confirm Password**—Enter the Password again for verification.

Step 4 Click **Apply** to save the changes to the running configuration.

Configuring L2TP over IPSec

This chapter describes how to use ASDM to configure L2TP over IPSec on the security appliance, and includes the following topics:

L2TP Overview

Layer 2 Tunneling Protocol (L2TP) is a VPN tunneling protocol which allows remote clients to use the public IP network to securely communicate with private corporate network servers. L2TP uses PPP over UDP (port 1701) to tunnel the data.

L2TP protocol is based on the client/server model. The function is divided between the L2TP Network Server (LNS), and the L2TP Access Concentrator (LAC). The LNS typically runs on a network gateway such as a router, while the LAC can be a dial-up Network Access Server (NAS), or a PC with a bundled L2TP client such as Microsoft Windows 2000.

The primary benefit of configuring L2TP with IPSec in a remote access scenario is that remote users can access a VPN over a public IP network without a gateway or a dedicated line, enabling remote access from virtually anyplace with POTS. An additional benefit is that the only client requirement for VPN access is the use of Windows 2000 with Microsoft Dial-Up Networking (DUN). No additional client software, such as Cisco VPN client software, is required.

The configuration of L2TP with IPSec supports certificates using the pre-shared keys or RSA signature methods, and the use of dynamic (as opposed to static) crypto maps. This summary of tasks assumes completion of IKE, as well as pre-shared keys or RSA signature configuration.

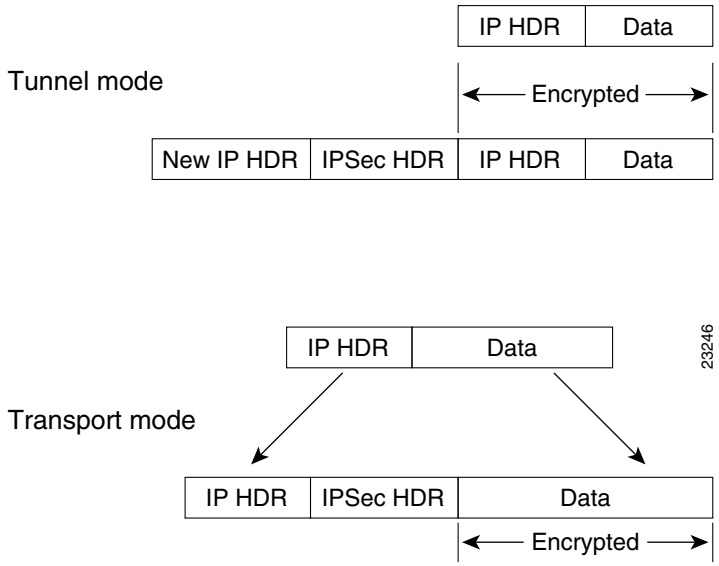
Note L2TP with IPSec on the security appliance allows the LNS to interoperate with the Windows 2000 L2TP client. Interoperability with LACs from Cisco and other vendors is currently not supported. Only L2TP with IPSec is supported, native L2TP itself is not supported on security appliance.
The minimum IPSec security association lifetime supported by the Windows 2000 client is 300 seconds. If the lifetime on the security appliance is set to less than 300 seconds, the Windows 2000 client ignores it and replaces it with a 300 second lifetime.

IPSec Transport and Tunnel Modes

By default, the security appliance uses IPSec tunnel mode—the entire original IP datagram is encrypted, and it becomes the payload in a new IP packet. This mode allows a network device, such as a router, to act as an IPSec proxy. That is, the router performs encryption on behalf of the hosts. The source router encrypts packets and forwards them along the IPSec tunnel. The destination router decrypts the original IP datagram and forwards it on to the destination system. The major advantage of tunnel mode is that the end systems do not need to be modified to receive the benefits of IPSec. Tunnel mode also protects against traffic analysis; with tunnel mode, an attacker can only determine the tunnel endpoints and not the true source and destination of the tunneled packets, even if they are the same as the tunnel endpoints.

However, the Windows 2000 L2TP/IPSec client uses IPSec transport mode—only the IP payload is encrypted, and the original IP headers are left intact. This mode has the advantages of adding only a few bytes to each packet and allowing devices on the public network to see the final source and destination of the packet. Figure 10-1 illustrates the differences between IPSec Tunnel and Transport modes.

Figure 10-1 IPSec in Tunnel and Transport Modes



Therefore, In order for Windows 2000 L2TP/IPSec clients to connect to the security appliance, you must configure IPSec transport mode for a transform (see Step 1). With this capability (transport), you can enable special processing (for example, QoS) on the intermediate network based on the information in the IP header. However, the Layer 4 header will be encrypted, limiting the examination of the packet. Unfortunately, transmitting the IP header in clear text, transport mode allows an attacker to perform some traffic analysis.

Note The security appliance does not establish an L2TP/IPSec tunnel with Windows 2000 if either the Cisco VPN Client Version, version 3.x or version 2.5, is installed. Disable the *Cisco VPN Service* for the Cisco VPN Client Version 3.x, or the *ANetIKE Service* for the Cisco VPN Client Version 2.5 from the Services panel in Windows 2000 (click **Start > Programs > Administrative Tools > Services**). Then restart the IPSec Policy Agent Service from the **Services** panel, and reboot the machine.

Configuring L2TP over IPSec

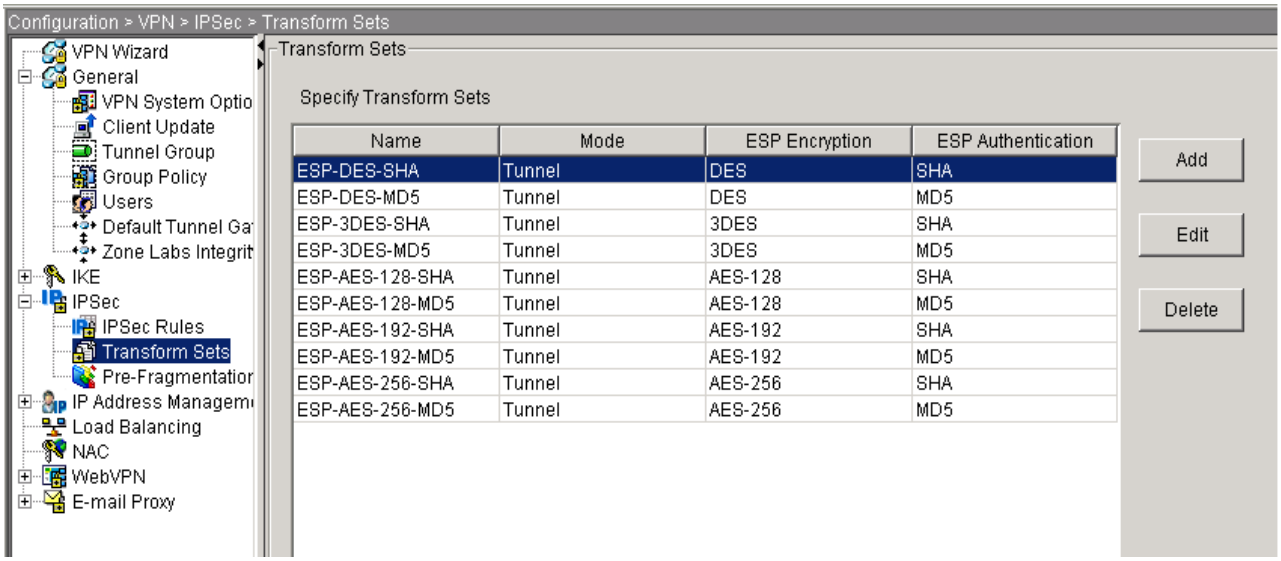
To configure the security appliance to accept L2TP over IPSec connections, follow these steps:

Note The security appliance does not establish an L2TP/IPSec tunnel with Windows 2000 if either the Cisco VPN Client Version 3.x or the Cisco VPN 3000 Client Version 2.5 is installed. Disable the *Cisco VPN Service* for the Cisco VPN Client Version 3.x, or the *ANetIKE Service* for the Cisco VPN 3000 Client Version 2.5 from the Services panel in Windows 2000 (choose **Start > Programs > Administrative Tools > Services**). Then restart the IPSec Policy Agent Service from the **Services** panel, and reboot the machine.

Step 1 Add an IPSec transform set, and specify IPSec to use transport mode rather than tunnel mode.

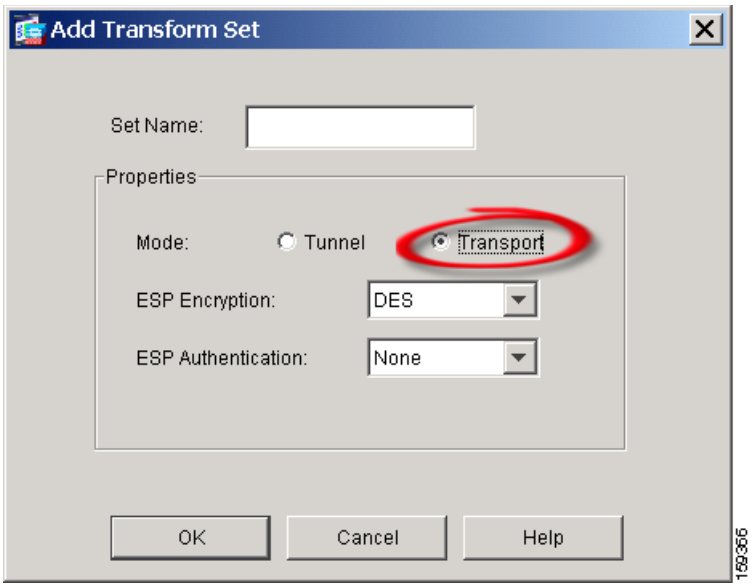
To do this, choose **Configuration > VPN > IPSec > Transform Sets**. Click **Add**. The Transform Sets pane displays (Figure 10-2).

Figure 10-2 Transform Sets Pane



Click **Add**. The Add Transform Set dialog displays (Figure 10-3).

Figure 10-3 Add Transform Set Dialog

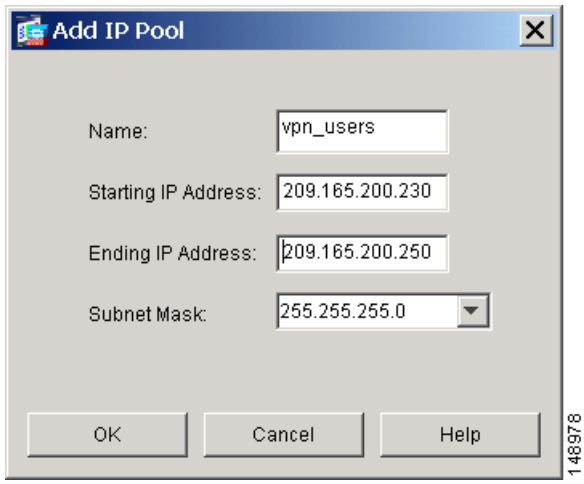


Enter a name for the transform set. Select the ESP Encryption and ESP Authentication methods. Click **OK**.

Step 2 Configure a method of address assignment. This example uses IP address pools.

To create an IP address pool, choose **Configuration > VPN > IP Address Management > IP Pools**. Click **Add**. The Add IP Pool dialog appears (Figure 10-4).

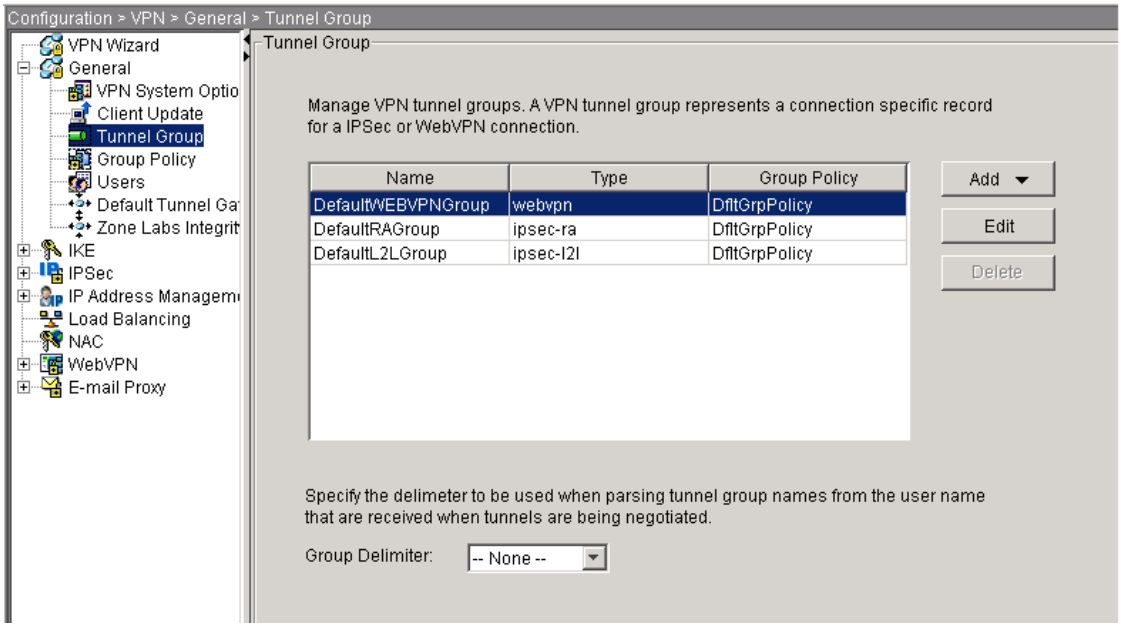
Figure 10-4 Add IP Pool Dialog



Enter the name of the new IP address pool. Enter the starting and ending IP addresses, and enter the subnet mask and click **OK**.

Step 3 Assign the IP address pool to a tunnel group. To do this, choose **Configuration >VPN > General > Tunnel Group**. The Tunnel Group pane appears (Figure 10-5):

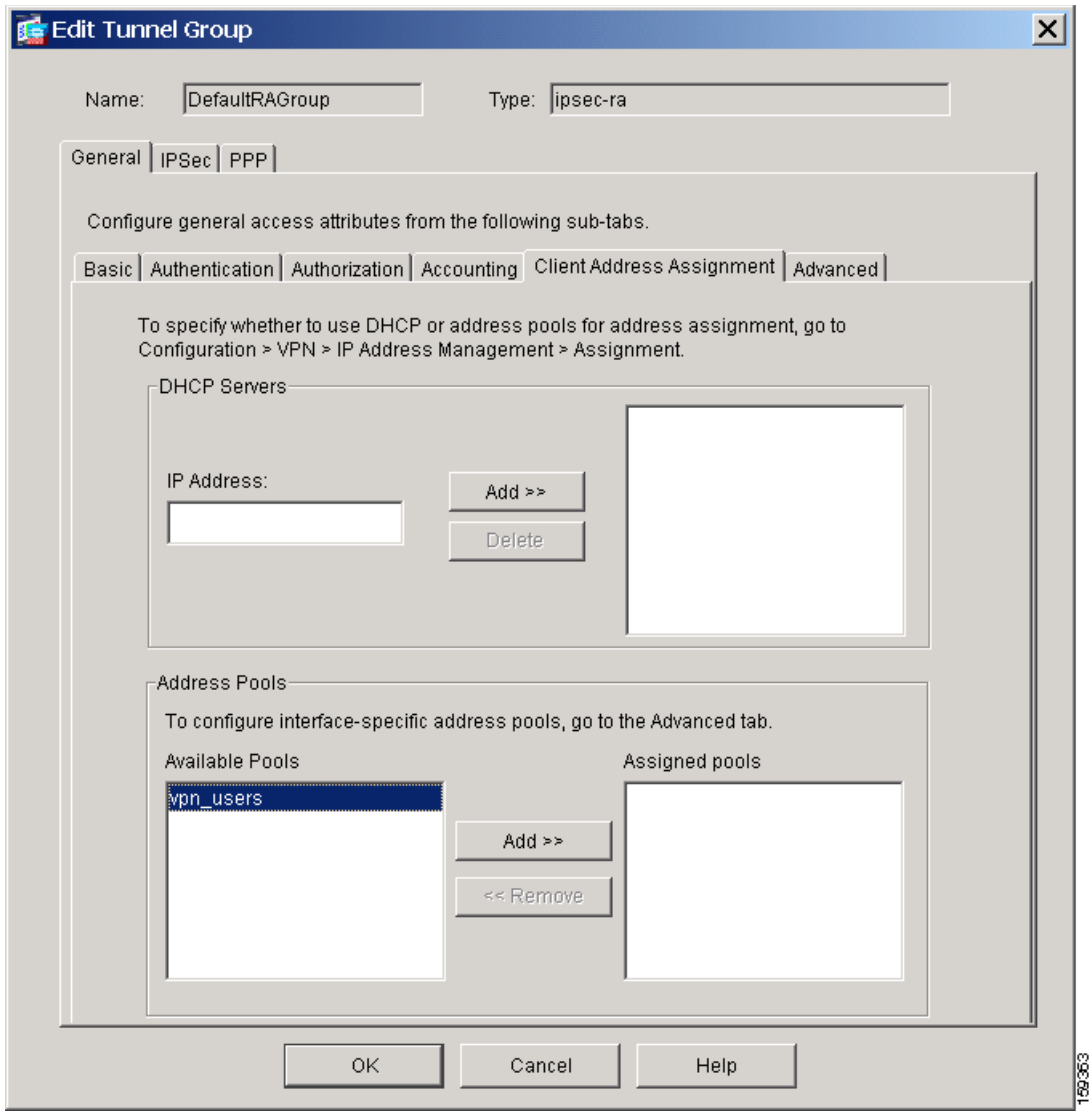
Figure 10-5 Tunnel Group Pane



Select a tunnel group in the table, and click **Edit.** The Edit Tunnel Group dialog appears.

Click the **Client Address Assignment** tab. The Client Address Assignment tab displays (Figure 10-6), containing the Address Pools group box.

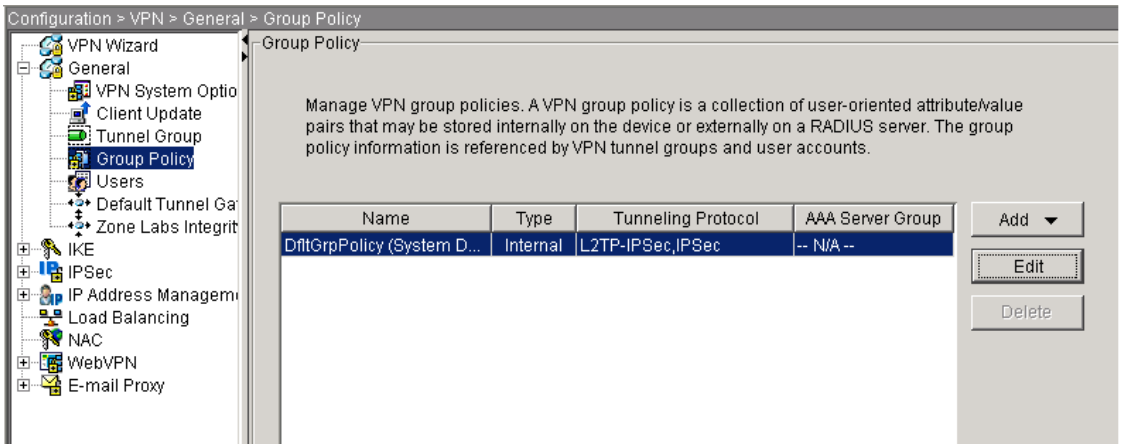
Figure 10-6 Edit Tunnel Group, General Tab, Client Address Assignment Tab



In the Address Pools area, choose an address pool to assign to the tunnel group and click **Add**. The address pool appears in the Assigned pools box.

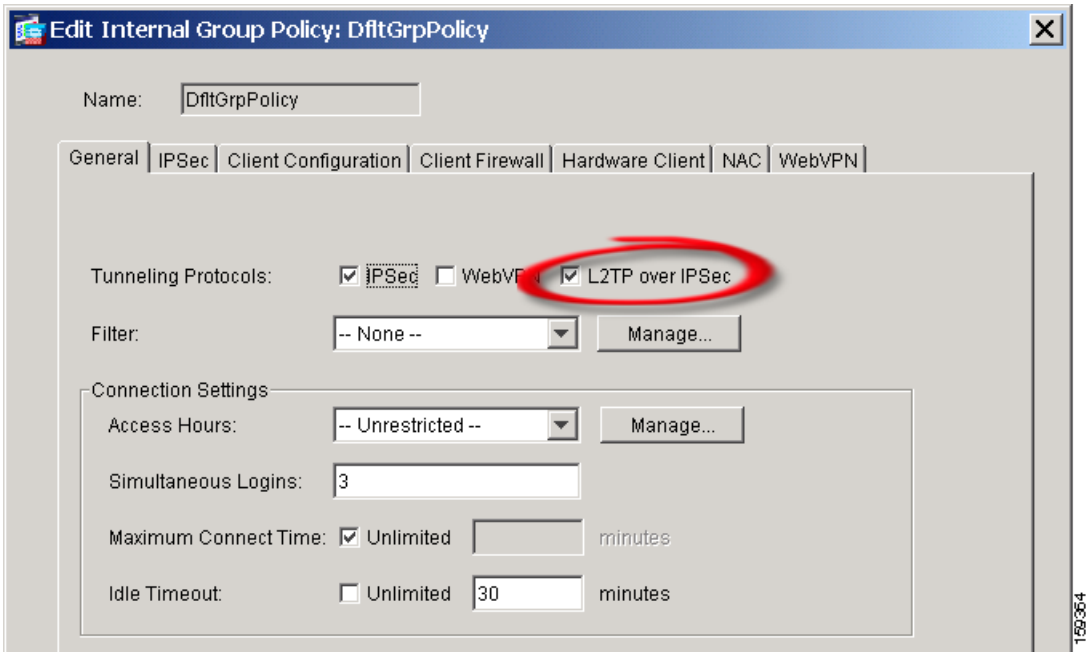
Step 4 Configure L2TP over IPSec as a valid VPN tunneling protocol for the group policy. Choose **Configuration > VPN > General > Group Policy.** The Group Policy pane displays (Figure 10-7).

Figure 10-7 Edit Internal Group Policy



Select a group policy, and click Edit. The Edit Group Policy dialog displays (Figure 10-8).

Figure 10-8 Edit Group Policy Dialog, General Tab



Click **L2TP over IPSec** to enable the protocol for the group policy. Click **OK**.

Step 5 Link the group policy to the tunnel group and enable Tunnel Group Switching (optional). Go back to the tunnel group configuration by choosing **Configuration >VPN > General > Tunnel Group**. The Tunnel Group pane appears. Choose the tunnel group and click **Edit**. The Edit Tunnel Group, General tab. Basic tab displays (Figure 10-9). Choose a group policy.

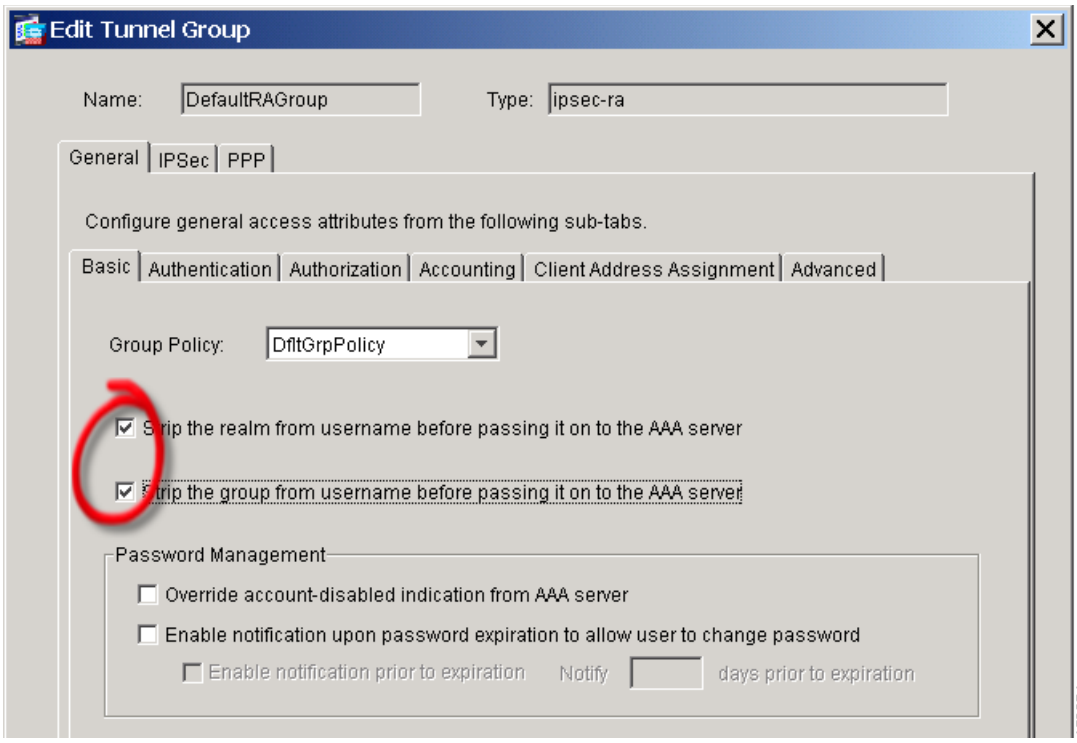
Tunnel Group Switching enables the security appliance to associate different users that are establishing L2TP over IPSec connections with different tunnel groups. Since each tunnel group has its own AAA server group and IP address pools, users can be authenticated through methods specific to their tunnel group.

With this feature, instead of sending just a username, the user sends a username and a group name in the format *username@group_name*, where "@" represents a delimiter that you can configure, and the group name is the name of a tunnel group that has been configured on the security appliance.

Tunnel Group Switching is enabled is enabled by Strip Group processing, which enables the security appliance to select the tunnel group for user connections by obtaining the group name from the username presented by the VPN client. The security appliance then sends only the user part of the username for authorization and authentication. Otherwise (if disabled), the security appliance sends the entire username, including the realm.

To enable Tunnel Group Switching, check **Strip the realm from username before passing it on to the AAA server**, and check **Strip the group from username before passing it on to the AAA server**. Click **OK**.

Figure 10-9 Edit Tunnel Group Dialog, General Tab, Basic Tab



Step 6 L2TP over IPSec uses PPP authentication protocols. Specify the protocols that are permitted for PPP connections on the PPP tab of the tunnel group (Figure 10-10). Table 10-1 shows the types of PPP authentication, and their characteristics.

Figure 10-10 Edit Tunnel Group, PPP Tab

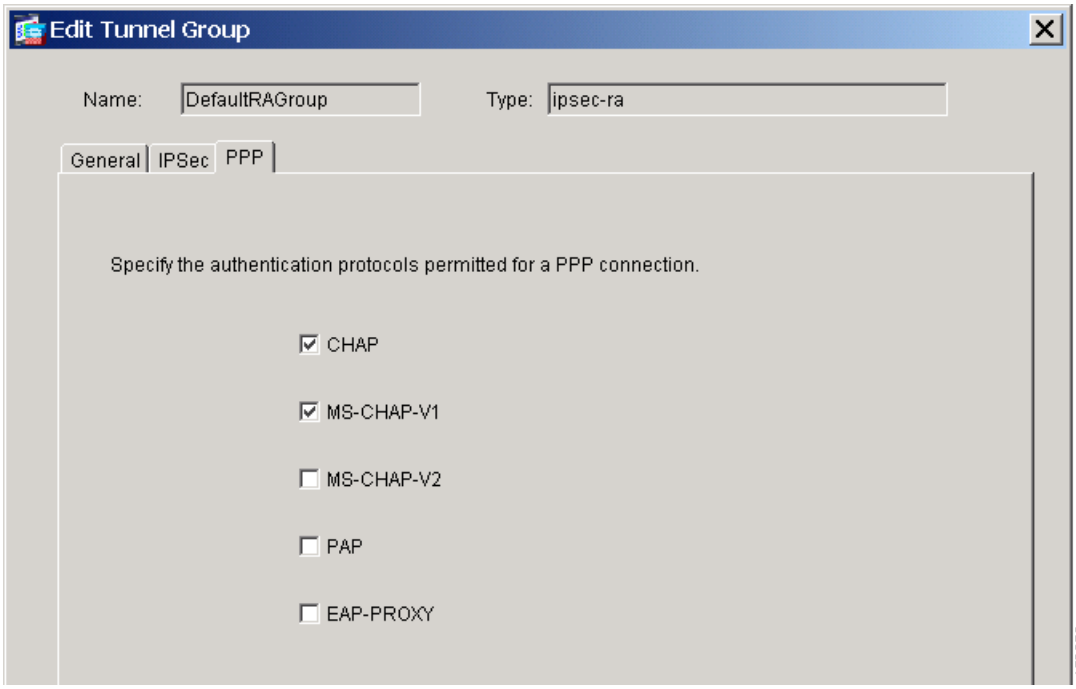


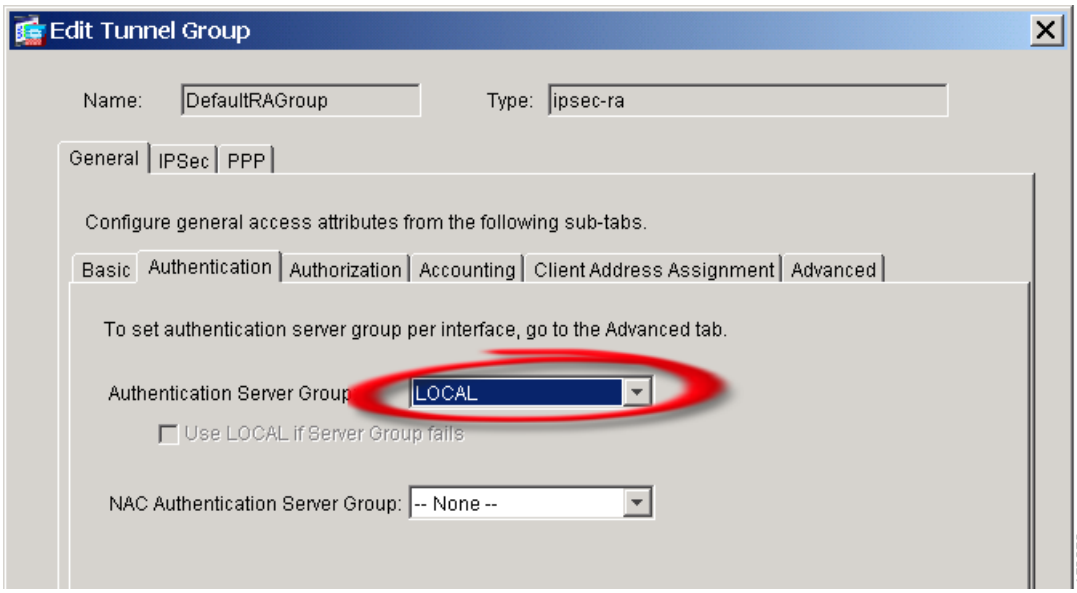
Table 10-1 Authentication Type Characteristics

Keyword	Authentication Type	Characteristics
chap	CHAP	In response to the server challenge, the client returns the encrypted [challenge plus password] with a clear text username. This protocol is more secure than the PAP, but it does not encrypt data.
eap-proxy	EAP	Enables EAP which permits the security appliance to proxy the PPP authentication process to an external RADIUS authentication server.
ms-chap-v1 **ms-chap-v2**	Microsoft CHAP, Version 1 Microsoft CHAP, Version, 2	Similar to CHAP but more secure in that the server stores and compares only encrypted passwords rather than clear text passwords as in CHAP. This protocol also generates a key for data encryption by MPPE.
pap	PAP	Passes clear text username and password during authentication and is not secure.

Step 7 Specify a method to authenticate users attempting L2TP over IPSec connections. You can configure the security appliance to use an authentication server or its own local database. Do do this, click the **Authentication** tab of the tunnel group. The Authentication tab displays (Figure 10-11).

By default, the security appliance uses its local database—the Authentication Server Group drop-down list displays LOCAL. To use an authentication server, select one from the list.

Figure 10-11 Edit Tunnel Group, General Tab, Authentication Tab

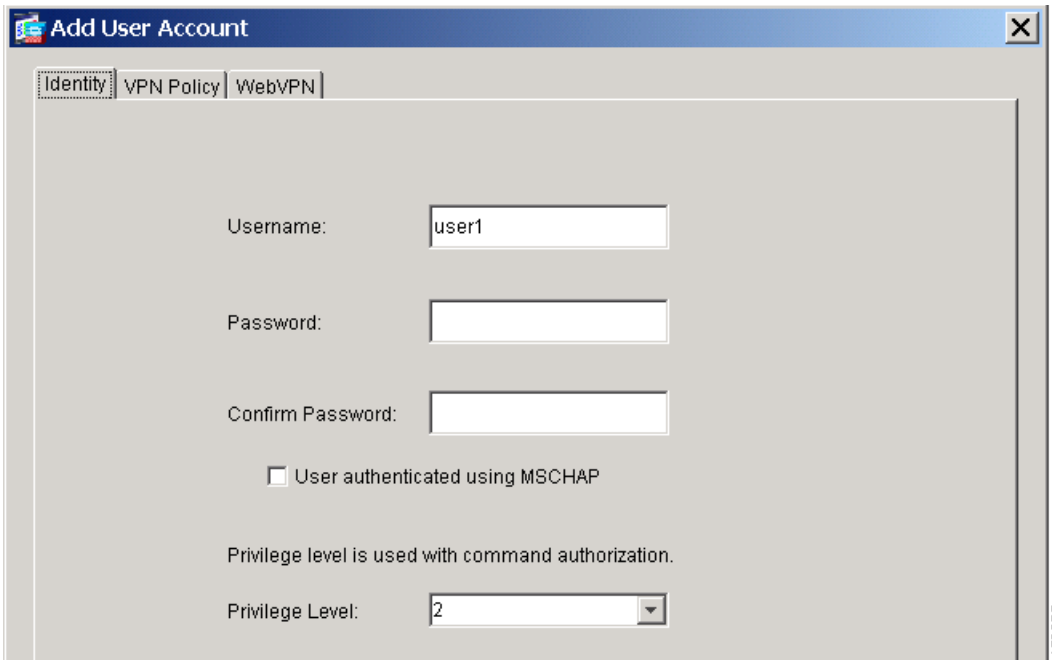


Note The security appliance only supports the PPP authentications PAP and Microsoft CHAP, Versions 1 and 2, on the local database. EAP and CHAP are performed by proxy authentication servers. Therefore, if a remote user belongs to a tunnel group configured with EAP or CHAP, and the security appliance is configured to use the local database, that user will not be able to connect.

Step 8 Create a user in the local database. Choose **Configuration >Properties > Device Administration > User Accounts.** Click **Add**. The Add User Accounts dialog opens (Figure 10-12).

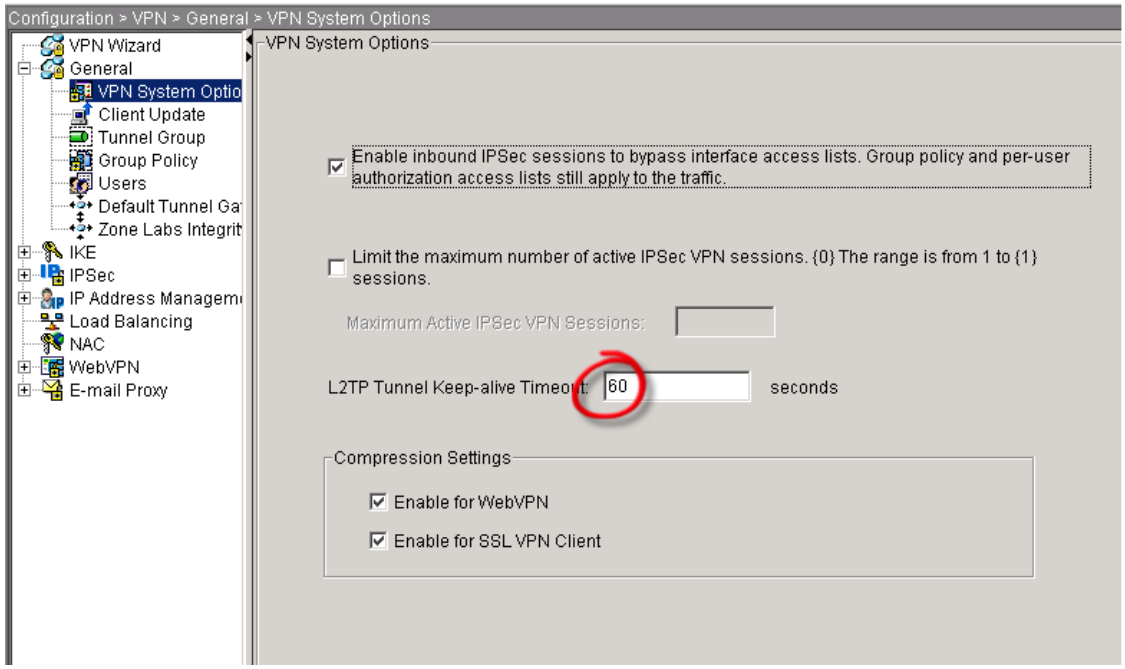
If the user is an L2TP client using Microsoft CHAP, Version 1 or Version 2, and the security appliance is configured to authenticate against the local database, you must enable the MSCHAP by clicking **User Authenticated using MSCHAP**.

Figure 10-12 Add User Account Dialog



Step 9 Configure the interval (in seconds) between hello messages. Choose **VPN > Configuration > General > VPN System Options**. The VPN System Options pane displays (Figure 10-13). Enter a value in seconds in the **L2TP Tunnel Keep-alive Timeout** field.

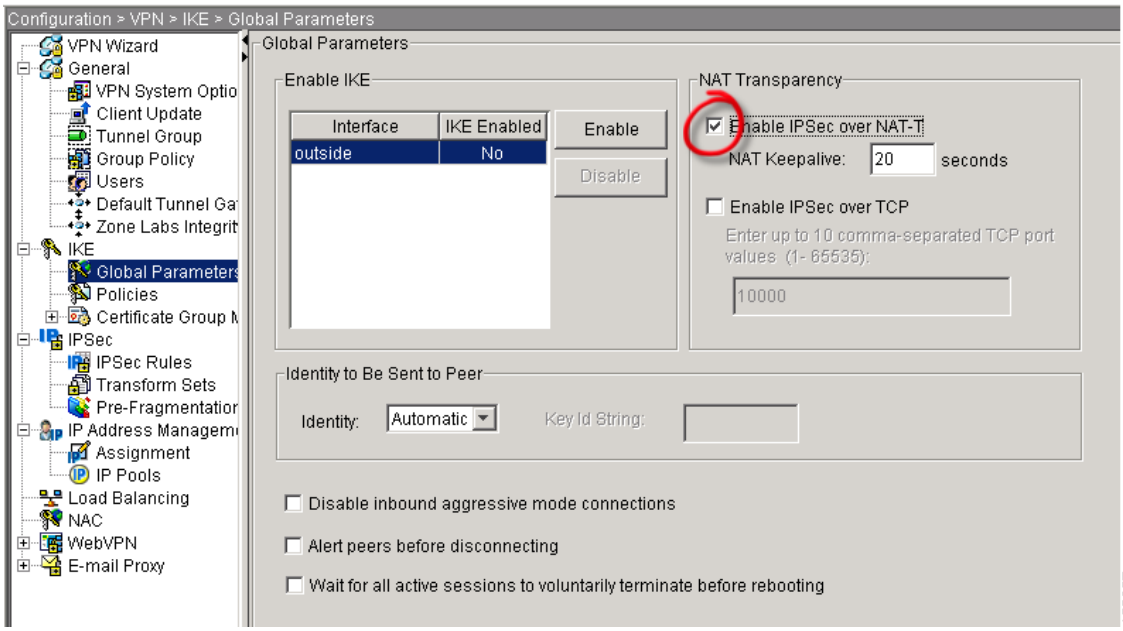
Figure 10-13 VPN System Options



Step 10 (Optional) If you expect multiple L2TP clients behind a NAT device to attempt L2TP over IPSec connections to the security appliance, you must enable NAT traversal so that ESP packets can pass through one or more NAT devices.

To do this, choose **Configuration > VPN > IKE > Global Parameters**. The IKE Global Parameters pane displays (Figure 10-14). Ensure that ISAKMP is enabled on an interface. Check **Enable IPSec over NAT-T** and click **OK**.

Figure 10-14 IKE Global Parameters Pane



Configuring Load Balancing

This chapter describes how to configure load balancing using ASDM. It include the following sections.

Introduction

If you have a remote-access configuration in which you are using two or more security appliances or VPN Concentrators connected on the same network to handle remote sessions, you can configure these devices to share their session load. This feature is called *load balancing*. To implement load balancing, group together logically two or more devices on the same private LAN-to-LAN network, private subnet, and public subnet into a *virtual cluster*.

All devices in the virtual cluster carry session loads. Load balancing directs session traffic to the least loaded device in the cluster, thus distributing the load among all devices. It makes efficient use of system resources and provides increased performance and high availability.

One device in the virtual cluster, the *virtual cluster master*, directs incoming traffic to the other devices, called *secondary 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 secondary devices in the cluster takes over that role and immediately becomes the new virtual cluster master.

The virtual cluster appears to outside clients 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; that is, it is a virtual address. 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 host in the cluster. In a second transaction (transparent to the user), the client connects directly to that host. In this way, the virtual cluster master directs traffic evenly and efficiently across resources.

Note All clients other than the Cisco VPN Client, Cisco VPN 3002 Hardware Client, or the Cisco ASA model 5505 when configured as a hardware client connect directly to the security appliance as usual; they do not use the virtual cluster IP address.

If a machine 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 another active device in the cluster. Should the virtual cluster master itself fail, another 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.

Implementing Load Balancing

Enabling load balancing involves:

- Configuring the load-balancing cluster by establishing a common virtual cluster IP address, UDP port (if necessary), and IPSec shared secret for the cluster. These values are identical for every device in the cluster.
- Configuring the participating device by enabling load balancing on the device and defining device-specific properties. These values vary from device to device.

Note VPN load balancing requires an active 3DES/AES license. The security appliance checks for the existence of this crypto license before enabling load balancing. If it does not detect an active 3DES or AES license, the security appliance prevents the enabling of load balancing and also prevents internal configuration of 3DES by the load balancing system, unless the license permits this usage.

Prerequisites

Load balancing is disabled by default. You must explicitly enable load balancing.

You must have first configured the public and private interfaces and also have previously configured the the interface to which the virtual cluster IP address refers.

All devices that participate in a cluster must share the same cluster-specific values: IP address, encryption settings, encryption key, and port.

Eligible Platforms

A load-balancing cluster can include security appliance models ASA 5520 and higher. You can also include VPN 3000 Series Concentrators in the cluster. While mixed configurations are possible, administration is generally simpler if the cluster is homogeneous.

Eligible Clients

Load balancing is effective only on remote sessions initiated with the following clients:

- Cisco VPN Client (Release 3.0 and later)
- Cisco VPN 3002 Hardware Client (Release 3.5 or later)
- Cisco ASA model 5505 when configured as a hardware client
- Cisco PIX 501/506E when acting as an Easy VPN client.

Load balancing works with both IPSec clients and WebVPN sessions. All other clients, including LAN-to-LAN connections, can connect to a security appliance on which load balancing is enabled, but they cannot participate in load balancing.

VPN Load-Balancing Cluster Configurations

A load-balancing cluster can consist of all ASA Release 7.0(x) security appliances, all ASA Release 7.1(1) security appliances or higher, all VPN 3000 Concentrators, or a mixture of these, subject to the following restrictions:

- Load-balancing clusters that consist of all ASA 7.0(x) security appliances, all ASA 7.1(1) security appliances or higher, or all VPN 3000 Concentrators can run load balancing for a mixture of IPSec and WebVPN sessions.
- Load-balancing clusters that consist of a both of ASA 7.0(x) security appliances and VPN 3000 Concentrators can run load balancing for a mixture of IPSec and WebVPN sessions.
- Load-balancing clusters that include ASA 7.1(1) security appliances or higher and either ASA 7.0(x) or VPN 3000 Concentrators or both can support only IPSec sessions. In such a configuration, however, the ASA 7.1(1) or higher security appliances might not reach their full IPSec capacity. Scenario 1: Mixed Cluster with No WebVPN Connections, page 11-4, illustrates this situation.

With Release 7.1(1) and higher, IPSec and WebVPN sessions count or weigh equally in determining the load that each device in the cluster carries. This represents a departure from the load balancing calculation for the ASA Release 7.0(x) software and the VPN 3000 Concentrator, in that these platforms both use a weighting algorithm that calculates 1 WebVPN session as equivalent in load to 10 IPSec sessions.

The virtual master of the cluster assigns session loads to the members of the cluster. An ASA Release 7.1(1) or higher security appliance regards all sessions, WebVPN or IPSec, as equal and assigns them accordingly. An ASA Release 7.0(x) security appliance or a VPN 3000 Concentrator performs the 10:1 weighting calculations in assigning session loads.

If you have a mixed configuration—that is, if your load-balancing cluster includes devices running a mixture of ASA software releases or at least one security appliance running ASA Release 7.1(1) or higher and a VPN 3000 Concentrator—the difference in weighting algorithms becomes an issue if the initial cluster master fails and another device takes over as master.

Suppose, for example, a security appliance running ASA Release 7.1(1) software is the initial cluster master. Then that device fails. Another device in the cluster takes over automatically as master and applies its own load-balancing algorithm to determine processor loads within the cluster. A cluster master running ASA Release 7.1(1) software cannot weight session loads in any way other than what that software provides. Therefore, it cannot assign a combination of IPSec and WebVPN session loads properly to ASA devices running earlier versions nor to VPN 3000 Concentrators. Conversely, a VPN 3000 Concentrator acting as the cluster master cannot assign loads properly to an ASA Release 7.1(1) security appliance. Scenario 2: Mixed Cluster Handling WebVPN Connections, page 11-4, illustrates this dilemma.

Note You can configure the number of IPSec and WebVPN sessions to allow, up to the maximum allowed by your configuration and license. See Configuring VPN Session Limits, page 11-6 for a description of how to set these limits.

Mixed Cluster Scenarios

The following scenarios illustrate the use of VPN load balancing in clusters consisting of a mixture of security appliances running ASA Release 7.1(1) or higher and ASA Release 7.0(x) software, as well as VPN 3000 Series Concentrators.

Scenario 1: Mixed Cluster with No WebVPN Connections

In this scenario, the cluster consists of a mixture of security appliances and VPN 3000 Concentrators. Some of the security appliance cluster peers are running ASA Release 7.0(x), and some are running Release 7.1(1) or higher. The pre-7.1(1) and VPN 3000 peers do not have any SSL VPN connections, and the 7.1(1) or higher cluster peers have only the base SSL VPN license, which allows two WebVPN sessions, but there are no SSL VPN connections. In this case, all the connections are IPSec, and load balancing works fine.

The two WebVPN licenses have a very small effect on the user's taking advantage of the maximum IPSec session limit, and then only when a VPN 3000 Concentrator is the cluster master. In general, the smaller the number of WebVPN licenses is on a security appliance in a mixed cluster, the smaller the effect on the ASA 7.1(1) or higher device being able to reach its IPSec session limit in a scenario where there are only IPSec sessions.

Scenario 2: Mixed Cluster Handling WebVPN Connections

This scenario is similar to the previous one, in that the cluster consists of a mixture of security appliances and VPN 3000 Concentrators. Some of the security appliance cluster peers are running ASA Release 7.0,(x) and some are running Release 7.1(1) or higher. In this case, however, the cluster is handling SSL VPN connections as well as IPSec connections.

If a device that is running software earlier than ASA Release 7.1(1) is the cluster master, the master applies the protocol and logic in effect prior to Release 7.1(1). That is, sessions might be directed to load-balancing peers that have exceeded their session limit. In that case, the user is denied access.

If the cluster master is a device running ASA Release 7.0(x) software, the old session-weighting algorithm applies only to the pre-7.1(1) peers in the cluster. No one should be denied access in this case. Because the pre-7.1(1) peers use the session-weighting algorithm, they are more lightly loaded.

An issue arises, however, because you cannot guarantee that the 7.1(1) or higher peer is always the cluster master. If the cluster master fails, another peer assumes the role of master. The new master might be any of the eligible peers. Because of the innately unpredictability of the results, we recommend that you avoid configuring this type of cluster.

Configuring Load Balancing

To configure load balancing on a security appliance running ASA Release 7.1(1) or higher software, configure the following elements for each device that participates in the cluster.

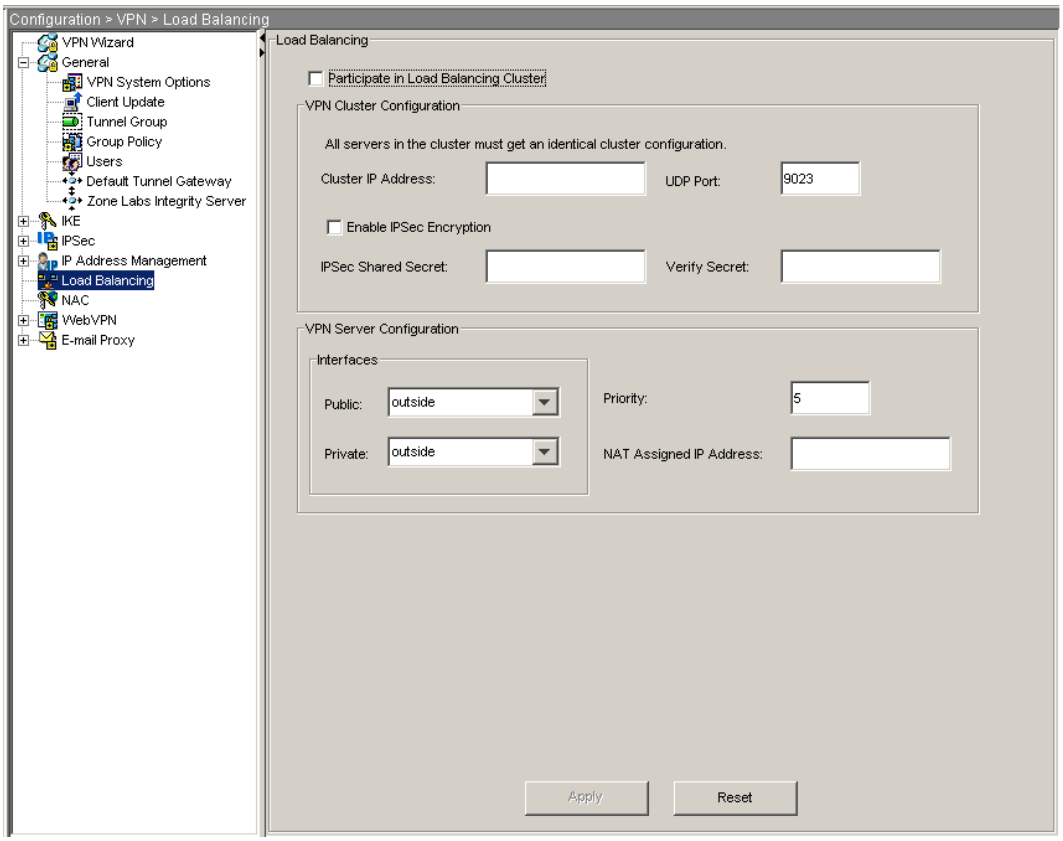
- Public and private interfaces
- VPN load-balancing cluster attributes

Note All participants in the cluster must have an identical cluster configuration, except for the device priority within the cluster.

Configuring the Public and Private Interfaces for Load Balancing

To configure a load-balancing cluster, select **Configuration > VPN > Load Balancing** (Figure 11-1).

Figure 11-1 Load Balancing Window



To configure load balancing, do the following steps:

Step 1 Check the Participate in Load Balancing check box.

Step 2 Configure the attributes in the VPN Cluster Configuration area, as follows:

Note All servers in the cluster must have an identical cluster configuration.

a. Enter the **Cluster IP Address**. This is the single IP address that represents the entire virtual cluster. Choose an IP address that is within the public subnet address range shared by all the security appliances in the virtual cluster.

b. Specify the **UDP Port** for the virtual cluster in which this device participates. The default value is 9023. If another application is using this port, enter the UDP destination port number you want to use for load balancing.

c. Optionally, enable IPSec encryption for the cluster by checking the check box for **Enable IPSec Encryption**. The default is no encryption. This attribute enables or disables IPSec encryption. If you configure this attribute, you must also specify and verify a shared secret.The security appliances in the virtual cluster communicate via LAN-to-LAN tunnels using IPSec. To ensure that all load-balancing information communicated between the devices is encrypted, enable this attribute.

Note When using encryption, you must have previously configured the load-balancing inside interface. If that interface is not enabled, an error message appears when you try to configure cluster encryption.

If the load-balancing inside interface was enabled when you configured cluster encryption, but was disabled before you configured the participation of the device in the virtual cluster, you get an error message when you select the Participate in Load Balancing Cluster check box, and encryption is not enabled for the cluster.

d. If you enable cluster encryption, you must also specify the IPSec shared secret by entering a value in the **IPSec Shared Secret** field, then entering the same value in the **Verify Secret** field. These fields must match. This command specifies the shared secret to between IPSec peers when you have enabled IPSec encryption. The value you enter in the field appears as consecutive asterisk characters

Step 3 Configure the attributes in the VPN Server Configuration area, as follows:

a. Select the **Public** interface on the security appliance. This command specifies the name or IP address of the public interface for load balancing for this device. The default value is outside.

b. Select the **Private** interface on the security appliance. This command specifies the name or IP address of the private interface for load balancing for this device. The default value is inside.

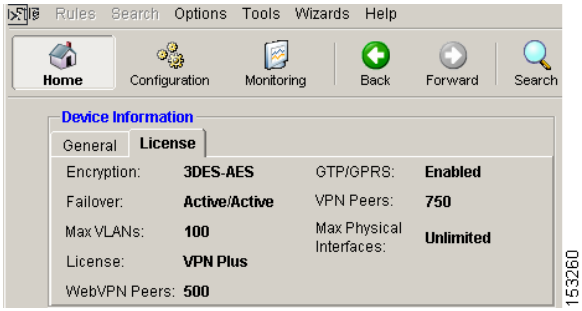
c. Set the priority to assign to this device within the cluster. The range is from 1 to 10. The priority indicates the likelihood of this device becoming the virtual cluster master, either at start-up or when an existing master fails. The higher you set the priority (for example, 10), the more likely it is that this device becomes the virtual cluster master.

d. If you want to apply network address translation for this device, enter the NAT Assigned IP Address for the device.

Configuring VPN Session Limits

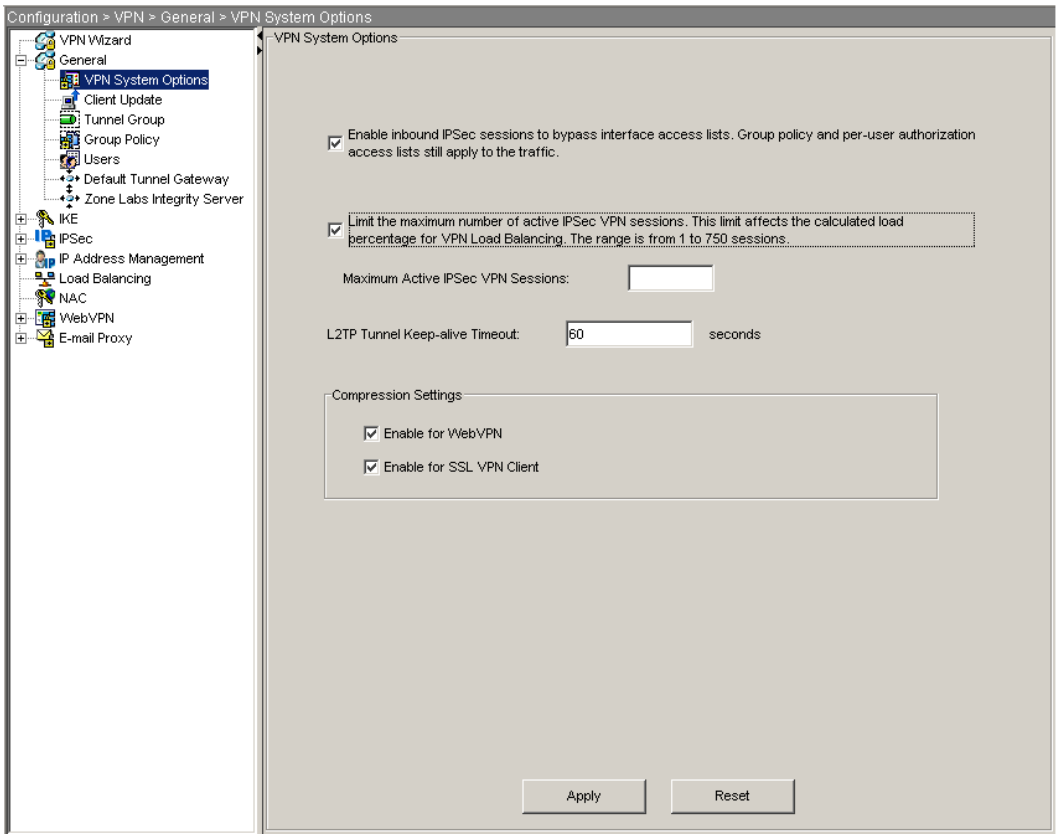
You can run as many IPSec and WebVPN sessions as your platform and license for the security appliance supports. To view the licensing information for your security appliance, select the Home icon at the top of the opening window for ASDM and select the License tab (Figure 11-2).

Figure 11-2 License Information



To limit the maximum number of active IPSec VPN sessions to a lower value than the security appliance allows, select **Configuration > VPN > General > VPN System Options** (Figure 11-3).

Figure 11-3 VPN System Options Window



Specify the limit that you want to apply in the **Maximum Active IPSec VPN Sessions** field. The maximum number of sessions depends on your license. This limit affects the calculated load percentage for VPN Load Balancing.

For example, if the security appliance license allows 750 IPSec sessions, and you want to limit the number of IPSec sessions to 500, enter 500 in the **Maximum Active IPSec VPN Sessions** field.

To remove the session limit, clear the **Limit the maximum number of active IPSec VPN sessions** check box.

For a complete description of the features available with each license, see *Cisco Security Appliance Command Line Configuration Guide*, Appendix A, "Feature Licenses and Specifications."

Configuring Easy VPN Services on the ASA 5505

This chapter describes how to use ASDM to configure the ASA 5505 as an Easy VPN hardware client. This chapter assumes you have configured the switch ports and VLAN interfaces of the ASA 5505 (see "Configuring Switch Ports and VLAN Interfaces for the Cisco ASA 5505 Adaptive Security Appliance" in the *Cisco Security Appliance Command Line Configuration Guide*).

Note The Easy VPN hardware client configuration specifies the IP address of its primary and secondary (backup) Easy VPN servers. Any ASA, including another ASA 5505 configured as a headend, a VPN 3000 Series Concentrator, an IOS-based router, or a firewall can act as an Easy VPN server. An ASA 5505 cannot, however function as both a client and a server simultaneously. To configure an ASA 5505 as a server, see "Specifying the Client/Server Role of the Cisco ASA 5505" on page 12-4. Then configure the ASA 5505 as you would any other ASA, beginning with the "Getting Started" chapter in the *Cisco Security Appliance Command Line Configuration Guide*.

This chapter includes the following sections:

Comparing Tunneling Options

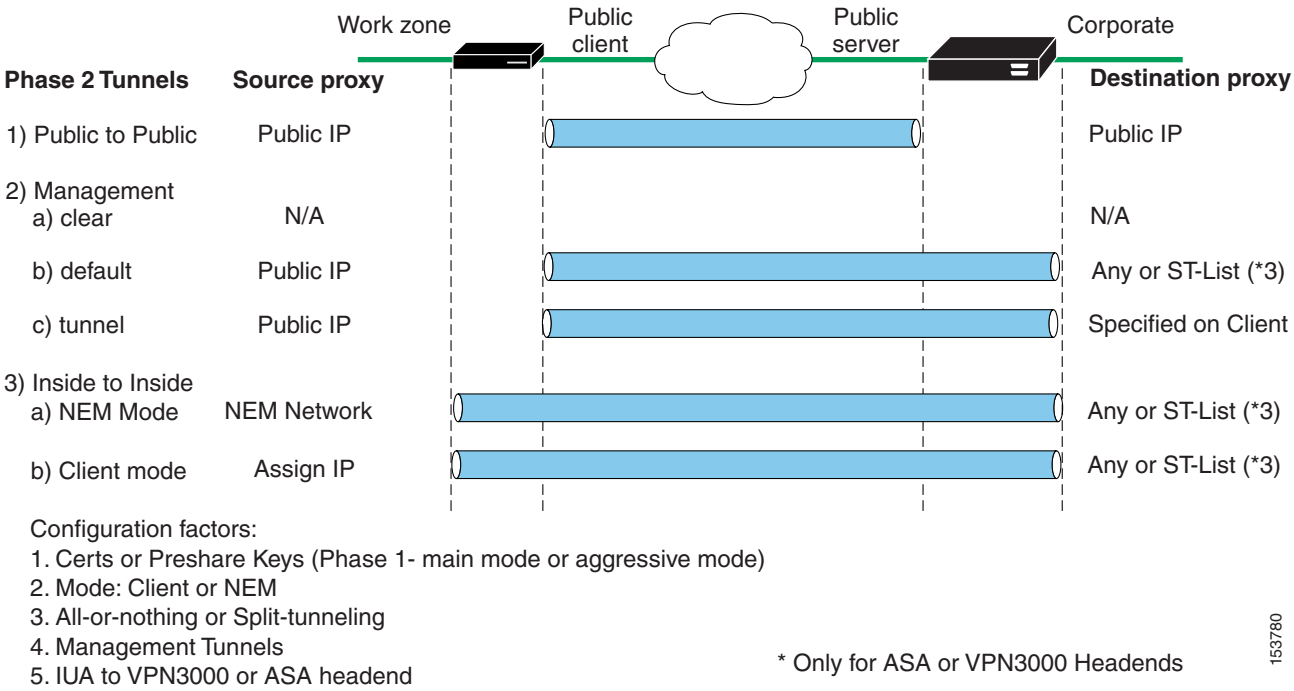
The tunnel types the Cisco ASA 5505 configured as an Easy VPN hardware client sets up depends on a combination of the following factors:

- You can use the Enable Tunneled Management attribute to automate the establishment of IPSec tunnels for remote management in addition to the data tunnel, the Clear Tunneled Management attribute to use normal routing to provide management access, or neither attribute to use IPSec to set up management tunnels in accordance with the Split Tunnel Policy and the Split Tunnel Network List attributes on the headend that permit, restrict, or prohibit split tunneling. (See "Configuring Tunneled Management" on page 12-11 for instructions on setting the Enable Tunneled Management and Enable Tunneled Management attributes, and "Configuring Client Configuration Parameters" on page 2-31 for instructions on setting the Split Tunnel Policy and the Split Tunnel Network List attributes on the headend.)

- Use of the Client Mode attribute to isolate the addresses of the inside hosts, relative to the client, from the enterprise network, or the network extension mode attribute to make those addresses accessible from the enterprise network.

Figure 12-1 shows the types of tunnels that the Easy VPN hardware client initiates, based on the combination of attribute settings.

Figure 12-1 Easy VPN Hardware Client Tunneling Options for the Cisco ASA 5505



The term “All-or-nothing” refers to the presence or absence of an access list for split tunneling. The access list distinguishes networks that require tunneling from those that do not.

Getting Started (Easy VPN Hardware Client Only)

Before configuring the ASA 5505 as an Easy VPN hardware client, you need to do the following:

- Retrieve one of the following sets of data, depending on the authentication method required by the server:
  - If the headend requires a preshared key for authentication, you need the tunnel group name and preshared key (that is, the group password). If the headend is an ASA, an ASDM connection to that headend displays the tunnel group name in the Configuration > VPN > General > Tunnel Group window. Double-click the tunnel group name and open the IPSec tab to view the Pre-shared key.
  - If the headend requires a trustpoint for authentication, you need the trustpoint name and whether sending the certificate chain is active. You also need to configure the trustpoint on the ASA 5505 that you are using as an Easy VPN hardware client. If the headend is an ASA, an ASDM connection to that headend displays the trustpoint name and certificate chain indicator in the

Configuration > VPN > General > Tunnel Group > Add or Edit tunnel > IPSec tab. Before proceeding, define the complementary trustpoint on the ASA 5505 that you are using as an Easy VPN hardware client, as described in the "Creating the Trustpoint" section on page 1-3.

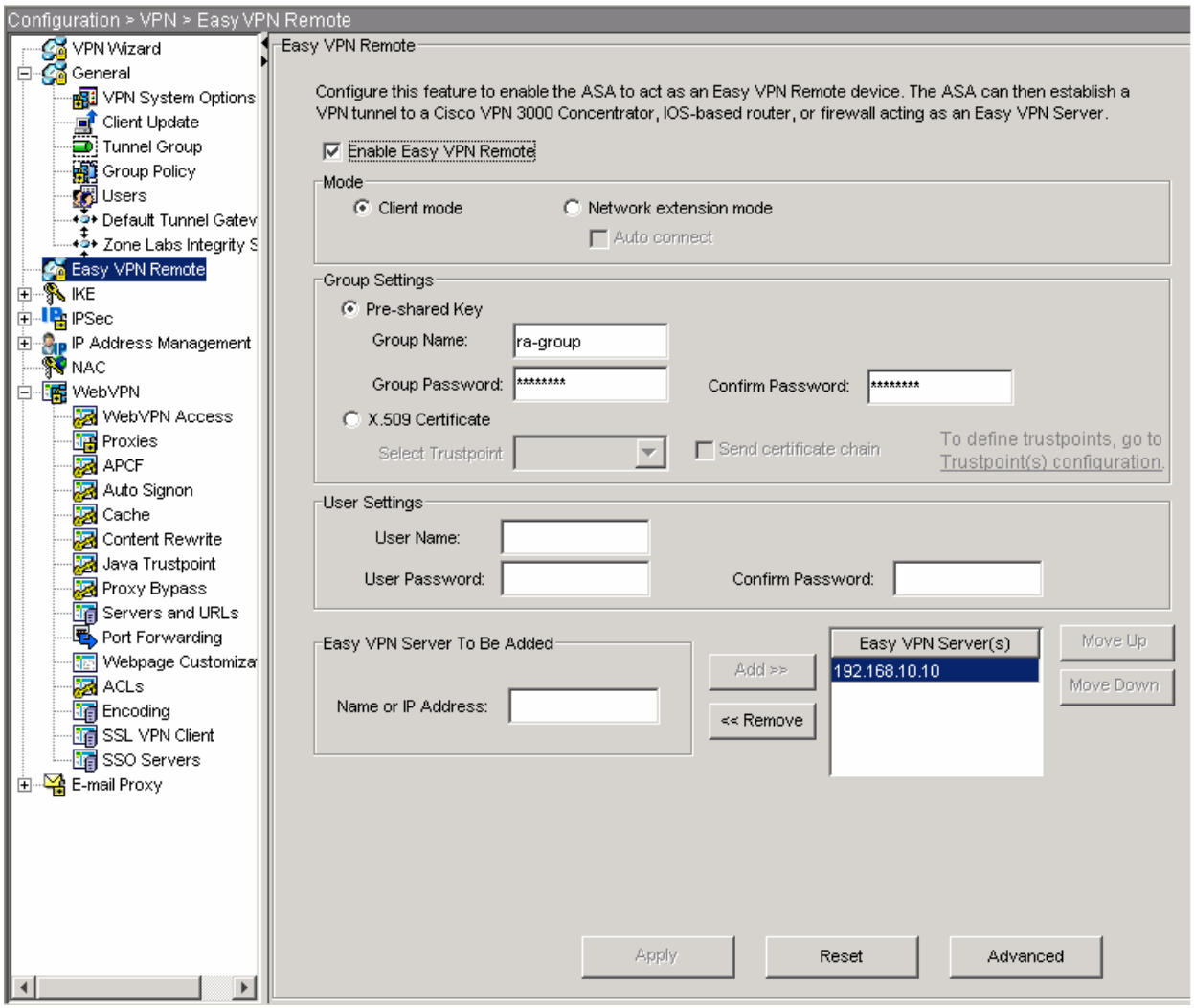
- (Optional) Retrieve the username and password from the server for the Easy VPN hardware client to use in response to an IKE Extended Authenticate (Xauth) challenge from the server.
- IP addresses of the primary and backup headends that will take the role of the Easy VPN servers.

Configuring Basic Settings

The basic settings for the Cisco ASA 5505 determine whether it functions as an Easy VPN hardware client, and if so, whether it exposes or hides the IP addresses of the hosts on the inside network from those on the enterprise network, the group or user security settings it uses to establish a connection to the headend, and the primary and backup headends to which it connects.

To configure the basic settings, choose Configuration > VPN > Easy VPN Remote. The Easy VPN Remote window opens (Figure 12-2).

Figure 12-2 Easy VPN Remote



The following sections describe how to assign settings to the attributes displayed in this window.

Specifying the Client/Server Role of the Cisco ASA 5505

The Cisco ASA 5505 functions as a Cisco Easy VPN hardware client (also called "Easy VPN Remote") or as a server (also called a "headend"), but not both at the same time.

Specify the role of the ASA 5505 in the network as follows:

Step 1 Remove or disable the following objects only if you configured the ASA 5505 as a headend and want to change it to a hardware client:

- To remove all user-defined tunnel groups, choose Configuration > VPN > General > Tunnel Group, select each tunnel group that is not a default tunnel group and click **Delete**, then click **Apply**.
- To disable the IPSec over TCP global IKE setting, choose Configuration > VPN > IKE > Global Parameters, uncheck IPSec over TCP, then click **Apply**.

- To remove the IKE policies, choose Configuration > VPN > IKE > Policies, select each policy and click **Delete**, then click **Apply**.
- To remove IPSec rules, choose Configuration > VPN > IPSec > IPSec Rules, select each rule and click **Delete**, then click **Apply**.
- To disable WebVPN, choose Configuration > VPN > WebVPN > WebVPN Access, select each interface and click **Disable**, then click **Apply**.

Note ASDM displays an error window if the configuration contains conflicting objects, and you try to enable the ASA 5505 as an Easy VPN hardware client (called "Easy VPN Remote" in Step 3 below) and click Apply. The error window identifies the types of objects remaining in the configuration that must be removed before you can successfully save the Easy VPN Remote setting to the configuration.

Step 2 Choose Configuration > VPN > Easy VPN Remote.

The Easy VPN Remote window opens (Figure 12-2).

Step 3 Do one of the following:

- Check **Easy VPN Remote** to specify the role of the ASA 5505 in the network as an Easy VPN hardware client.
- Uncheck **Easy VPN Remote** to specify the role of the ASA 5505 in the network as a headend.

  ASDM dims the remaining attributes in this window if you uncheck this attribute.

Note If you uncheck this attribute, click **Apply**, then configure the ASA 5505 as you would any other ASA, beginning with the "Getting Started" chapter in the *Cisco Security Appliance Command Line Configuration Guide*. Disregard the remaining sections in this chapter.

With the exception of the User Settings area, ASDM requires that you assign settings to the remaining attributes in this window before you click Apply if you checked Easy VPN Remote. Complete the instructions in the sections that follow to assign settings to these attributes, then click **Apply** to save the changes to the running configuration.

Specifying the Mode

The Easy VPN hardware client supports one of two modes of operation: client mode or network extension mode. The mode of operation determines whether the IP addresses of the inside hosts relative to the Easy VPN hardware client are accessible from the Enterprise network over the tunnel. Specifying a mode of operation is mandatory before making a connection because the Easy VPN hardware client does not have a default mode.

Specify the mode of the Easy VPN hardware client as follows:

Step 1 Choose Configuration > VPN > Easy VPN Remote.

The Easy VPN Remote window opens (Figure 12-2).

Step 2 Check one of the following Mode options:

- **Client mode**—Also called port address translation (PAT) mode, client mode isolates the IP addresses of all devices on the Easy VPN hardware client private network from those on the enterprise network. The Easy VPN hardware client performs PAT for all VPN traffic for its inside hosts.

  Note IP address management is neither required for the Easy VPN hardware client inside interface nor the inside hosts.

- **Network extension mode** (NEM)—Makes the inside interface and all inside hosts routeable across the enterprise network over the tunnel. Hosts on the inside network obtain their IP addresses from an accessible subnet (statically or via DHCP) pre-configured with static IP addresses. PAT does not apply to VPN traffic in NEM. This mode does not require a VPN configuration for each client. The Cisco ASA 5505 configured for NEM supports automatic tunnel initiation. The configuration must store the group name, user name, and password. Automatic tunnel initiation is disabled if secure unit authentication is enabled.

  ASDM activates the Auto connect check box only if you check Network extension mode.

Step 3 Use the following instructions if you checked Network extension mode:

- **Auto connect**—The Easy VPN Remote establishes automatic IPSec data tunnels unless both of the following are true: Network extension mode is configured locally, and split-tunneling is configured on the group policy pushed to the Easy VPN Remote. If both are true, checking this attribute automates the establishment of IPSec data tunnels. Otherwise, this attribute has no effect.

Step 4 Click **Apply** only if the configuration of the Easy VPN Client is complete and you have opened the Easy VPN Remote window to modify attributes in the Mode area. Otherwise, continue with the remaining sections for the Easy VPN Remote window, then click **Apply**.

Note If the Easy VPN hardware client is using NEM and has connections to secondary servers, establish an ASDM connection to each headend, open the Configuration > VPN > IPSec > IPSec Rules > Tunnel Policy (Crypto Map) - Advanced tab on that ASDM connection, and check **Enable Reverse Route Injection** to configure dynamic announcements of the remote network using RRI.

Specifying a Tunnel Group or Trustpoint

When configuring the Cisco ASA 5505 as an Easy VPN hardware client, you can specify the pre-shared key or the name of the trustpoint configured on the Easy VPN server. See the section that names the option used for the authentication configured on the headend that you are using as the Easy VPN server:

- Specifying the Pre-shared Key
- Specifying the Trustpoint

Specifying the Pre-shared Key

Specify the pre-shared key of the Easy VPN hardware client to match that of the headend, as follows:

Step 1 Choose Configuration > VPN > Easy VPN Remote.

The Easy VPN Remote window opens (Figure 12-2).

Step 2 Click **Pre-shared Key** under Group Settings.

A description of this attribute follows:

- **Pre-shared key**—Indicates the use of an IKE pre-shared key for authentication and makes available the subsequent Group Name, Group Password, and Confirm Password fields for specifying the group policy name and password containing that key.

Step 3 Assign values to the following attributes:

- **Group Name**—Enter the name of the VPN tunnel group configured on the headend. You must configure this tunnel group on the server before establishing a connection.
- **Group Password**—Enter the IKE pre-shared key used for authentication on the headend.

Step 4 Click **Apply** only if the configuration of the Easy VPN Client is complete and you have opened the Easy VPN Remote window to modify the group settings. Otherwise, continue with the remaining sections for the Easy VPN Remote window, beginning with the "Configuring Automatic Xauth Authentication" section on page 12-8, then click **Apply**.

Specifying the Trustpoint

Specify the trustpoint configured on both the headend and the associated one on the Easy VPN hardware client you are configuring (see "Getting Started (Easy VPN Hardware Client Only)" on page 12-2), as follows:

Step 1 Choose Configuration > VPN > Easy VPN Remote.

The Easy VPN Remote window opens (Figure 12-2).

Step 2 Assign values to the following attributes in the Group Settings area of this window:

- **X.509 Certificate**—Click to indicate the use of an X.509 digital certificate, supplied by a Certificate Authority, for authentication.
- **Select Trustpoint**—Select the trustpoint identifying the RSA certificate to use for authentication. The trustpoint name can take the form of an IP address. To define a trustpoint to populate this drop-down list, click **Trustpoint(s) configuration** to the right.
- **Send certificate chain**—(Optional) Enables sending a certificate chain, not just the certificate itself. This action includes the root certificate and any subordinate CA certificates in the transmission.

Step 3 Click **Apply** only if the configuration of the Easy VPN Client is complete and you have opened the Easy VPN Remote window to modify the group settings. Otherwise, continue with the remaining sections for the Easy VPN Remote window, then click **Apply**.

Configuring Automatic Xauth Authentication

The ASA 5505 configured as an Easy VPN hardware client automatically authenticates when it connects to the Easy VPN server if all of the following conditions are true:

- Secure unit authentication is disabled on the server.
- The server requests IKE Extended Authenticate (Xauth) credentials.

  Xauth provides the capability of authenticating a user within IKE using TACACS+ or RADIUS. Xauth authenticates a user (in this case, the Easy VPN hardware client) using RADIUS or any of the other supported user authentication protocols.
- The client configuration contains an Xauth username and password.

Thus, configuring Xauth login credentials on the Easy VPN hardware client is optional.

Configure the Xauth login credentials, as follows:

Step 1 Choose Configuration > VPN > Easy VPN Remote.

The Easy VPN Remote window opens (Figure 12-2).

Step 2 Assign values to the following attributes in the Group Settings area of this window:

- **User Name**—Enter the user name that the Easy VPN hardware client can use in response to an Xauth challenge from the authentication server or headend. The name can be between 1 and 64 characters, but must be configured on the server or headend.
- **User Password**—Enter the password that the Easy VPN hardware client can use in response to an Xauth challenge from the authentication server or headend. The password can be between 1 and 64 characters, but must be configured on the server or headend.
- **Confirm Password**—Enter the User Password again for verification.

Step 3 Click **Apply** only if the configuration of the Easy VPN Client is complete and you have opened the Easy VPN Remote window to modify the user settings. Otherwise, continue with the next section, then click **Apply**.

Specifying the Addresses of the Easy VPN Servers

Before establishing a connection with an Easy VPN hardware client, you must specify the IP address of at least one headend to act as the Easy VPN server. Any ASA, including another ASA 5505 configured as a headend, a VPN 3000 Series Concentrator, an IOS-based router, or a firewall can act as an Easy VPN server.

Configure the IP addresses of the primary Easy VPN server and the Easy VPN servers that you would like to use as backups, as follows:

Step 1 Choose Configuration > VPN > Easy VPN Remote.

The Easy VPN Remote window opens (Figure 12-2).

Step 2 Use the following attribute description to assign a value in the Easy VPN Server To Be Added area of this window:

Name or IP Address—Enter the IP address or DNS name of the headend to serve as the primary Easy VPN server and click **Add**. ASDM inserts it into the Easy VPN Server(s) list. Repeat for each backup Easy VPN server.

Step 3 Select an entry and click **Move Up** or **Move Down** to prioritize the client connection attempt to the associated Easy VPN server.

Step 4 Select an entry and click **Remove** if you want to remove the associated Easy VPN server from the list.

Step 5 Click **Apply** to save the changes you made in this window to the running configuration.

Note The ASDM session retains the settings in the window if an error window identifies objects that conflict with the configuration of the ASA 5505 as an Easy VPN hardware client. The error window identifies the object types remaining in the configuration that must be removed before you can successfully save the changes in this window. After removing the conflicting objects, return to this window and click **Apply** again.

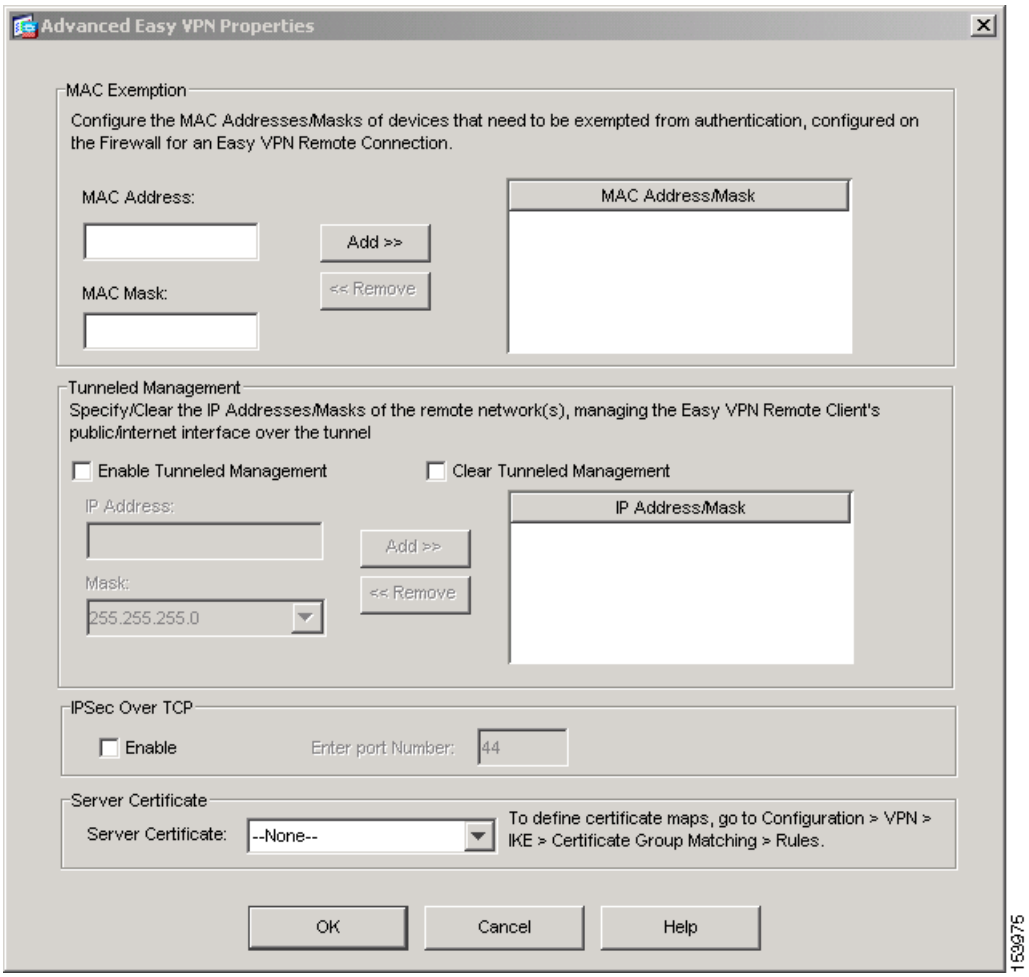
Configuring Advanced Settings

The advanced settings for the Easy VPN hardware client are optional. They let you do the following:

- Identify devices on the inside network to exclude from individual user authentication requirements.
- Automate the creation of IPSec tunnels to provide management access from the corporate network to the outside interface of the ASA 5505.
- Enable or disable TCP encapsulation of IPSec.
- Configure the Easy VPN hardware client to accept only connections to Easy VPN servers with digital certificates identified by a specified certificate map.

To configure the advanced settings for the Easy VPN hardware client, choose Configuration > VPN > Easy VPN Remote, then click **Advanced** at the bottom of the Easy VPN Remote window. ASDM opens the Advanced Easy VPN Remote Properties window (Figure 12-3).

Figure 12-3 Advanced Easy VPN Remote Properties



Note Each area is optional and is independent from the others; the attribute settings in one area do not require settings in another area of this window.

The following sections describe how to assign settings to the attributes in this window.

Configuring Device Pass-Through

Devices such as Cisco IP phones, wireless access points, and printers are incapable of performing authentication. If individual user authentication is enabled, use the following instructions to exempt such devices from authentication, thereby providing network access to them:

Step 1 Choose Configuration > VPN > Easy VPN Remote, then click **Advanced** at the bottom of the Easy VPN Remote window.

ASDM opens the Advanced Easy VPN Remote Properties window (Figure 12-3). The MAC Exemption area at the top of the window lets you configure device pass-through.

Step 2 Assign values to the following attributes:

- **MAC Address**—Enter the MAC address, in dotted hexadecimal notation, of the device for which you want to bypass individual user authentication.
- **MAC Mask**—Enter the network mask for the corresponding MAC address. A MAC mask of ffff.ff00.0000 matches all devices made by the same manufacturer. A MAC mask of ffff.ffff.ffff matches a single device.

Note You only need to enter the first six characters of the MAC address if you enter the MAC mask ffff.ff00.0000 to specify all devices by the same manufacturer. For example, Cisco IP phones have the Manufacturer ID 00036b, so entering `0003.6b00.0000` as the MAC address and `ffff.ff00.0000` as the MAC mask command exempts any Cisco IP phone, including Cisco IP phones you might add in the future. Entering the MAC address `0003.6b54.b213` and the MAC mask `ffff.ffff.ffff` provides greater security but less flexibility because it exempts one specific Cisco IP phone.

Step 3 Click **Add**.

ASDM inserts the MAC Address and MAC Mask into MAC Address/Mask list.

Step 4 Repeat Steps 2 and 3 for each additional device you want to exempt from user authentication requirements.

Step 5 Select an entry and click **Remove** if you want to remove the device from the list.

Step 6 Click **OK**, then **Apply** if these attributes are the only ones you are modifying in the Advanced Easy VPN Properties window. Otherwise, continue with the next section.

Configuring Tunneled Management

The Cisco ASA 5505, operating as an Easy VPN hardware client, supports management access using SSH or HTTPS, with or without a second layer of additional encryption. You can configure the Easy VPN hardware client to require IPSec encryption within the SSH or HTTPS encryption already present in management sessions.

Step 1 Choose Configuration > VPN > Easy VPN Remote, then click **Advanced** at the bottom of the Easy VPN Remote window.

ASDM opens the Advanced Easy VPN Remote Properties window (Figure 12-3).

Step 2 Choose one of the following options:

- **Enable Tunneled Management**—Check to automate the creation of IPSec tunnels to provide management access from the corporate network to the outside interface of the ASA 5505. The Easy VPN hardware client and server create management tunnels automatically when they create the data tunnel.
- **Clear Tunneled Management**—Check to use normal routing to provide management access from the corporate network to the outside interface of the ASA 5505 (no tunneling of management packets). Check this attribute if a NAT device is operating between the Easy VPN hardware client and the Internet.

- Leave both the **Enable Tunneled Management** and **Clear Tunneled Management** check boxes blank to set up IPSec for management tunnels in accordance with the **split-tunnel-policy** and **split-tunnel-network-list** commands.

Note Steps 3 through 6 apply only if you checked Enable Tunneled Management.

Step 3 See the descriptions to assign values to the following attributes:

- **IP Address**—Enter the IP address of the remote network or host to automate the creation of an IPSec tunnel for management access.
- **Mask**—Select the subnet mask associated with the IP address you entered.

Step 4 Click **Add**.

ASDM inserts the IP Address and mask into the IP Address/Mask list.

Step 5 Repeat Steps 3 and 4 for each additional network or host for which you want to automate the creation of an IPSec tunnel for remote management access.

Step 6 Select an entry and click **Remove** if you want to remove the device from the list.

Step 7 Click **OK**, then **Apply** if these attributes are the last or only ones you are modifying in the Advanced Easy VPN Properties window. Otherwise, continue with the next section.

Configuring IPSec over TCP

By default, the Easy VPN hardware client and server encapsulate IPSec in User Datagram Protocol (UDP) packets. Some environments, such as those with certain firewall rules, or NAT and PAT devices, prohibit UDP. To use standard Encapsulating Security Protocol (ESP, Protocol 50) or Internet Key Exchange (IKE, UDP 500) in such environments, you must configure the client and the server to encapsulate these packets within TCP packets to enable secure tunneling. If your environment allows UDP, however, configuring IPSec over TCP adds unnecessary overhead.

Enable or disable TCP encapsulation of IPSec, as follows:

Step 1 Choose Configuration > VPN > Easy VPN Remote, then click **Advanced** at the bottom of the Easy VPN Remote window.

ASDM opens the Advanced Easy VPN Remote Properties window (Figure 12-3).

Step 2 See the following description to set the attributes in the IPSec Over TCP area:

- **Enable (IPSec Over TCP)**—Check to use TCP to encapsulate IPSec over UDP packets. Uncheck to use UDP only.

  ASDM activates the Enter port Number box if you check this attribute.
- **Enter port Number**—Enter the port number to use for IPSec over TCP. By default, the Easy VPN hardware client uses port 10000, however, you must enter a port number if you checked Enable (IPSec Over TCP). Enter 10000, or use the same port number assigned on the headend.

Step 3 Click **OK**, then **Apply** if these attributes are the last or only ones you are modifying in the Advanced Easy VPN Properties window. Otherwise, continue with the next section.

Note Choose Configuration > VPN > IPSec > Pre-Fragmentation, double-click the outside interface, and set the DF Bit Setting Policy to Clear if you configure the Easy VPN Remote connection to use TCP-encapsulated IPSec. This action clears the Don't Fragment (DF) bit from the encapsulated header. A DF bit is a bit within the IP header that determines whether the packet can be fragmented. This command lets the Easy VPN hardware client send packets that are larger than the MTU size.

Configuring Certificate Filtering

You can configure the Easy VPN hardware client to accept only connections to Easy VPN servers with digital certificates identified by a specified certificate map. Before doing so, you must create the map, using the Configuration > VPN > IKE > Certificate Group Matching > Rules menu path. Then assign the certificate map, as follows:

Step 1 Choose Configuration > VPN > Easy VPN Remote, then click **Advanced** at the bottom of the Easy VPN Remote window.

ASDM opens the Advanced Easy VPN Remote Properties window (Figure 12-3).

Step 2 Use the following description to set the attribute at the bottom of the window:

- **Server Certificate**—Select the certificate map that identifies the certificates that you want the Easy VPN hardware client connections to support. The mapping names in the first table of the Rules window accessed by the Configuration > VPN > IKE > Certificate Group Matching > Rules menu path populate the drop-down list.

Step 3 Click **OK**, then **Apply**.

Guidelines for Configuring the Easy VPN Server

The following sections address the Easy VPN hardware client considerations that apply to the Easy VPN server:

- Authentication Options
- Group Policy and User Attributes Pushed to the Client

Authentication Options

The ASA 5505 supports the following authentication mechanisms, which it obtains from the group policy stored on the Easy VPN Server. The following list identifies the authentication options supported by the Easy VPN hardware client, however, you must configure them on the Easy VPN server:

- Require Interactive Client Authentication (Also called secure unit authentication) on the Configuration > VPN General > Group Policy > Add or Edit Internal Group Policy > Hardware Client tab

  When enabled, this attribute ignores the Xauth login credentials (described in "Configuring Automatic Xauth Authentication" on page 12-8) and requires the user to authenticate the ASA 5505 by entering a password.

- Require Individual User Authentication, also on the Hardware Client tab

  When enabled, this attribute requires users behind the ASA 5505 to authenticate before granting them access to the enterprise VPN network.

Caution Do not use IUA if the client might have a NAT device.

- User Authentication Idle Timeout, also on the Hardware Client tab

  This attribute sets or remove the idle timeout period after which the Easy VPN Server terminates the client's access.

- Authentication by HTTP redirection

  The Cisco Easy VPN server intercepts HTTP traffic and redirects the user to a login page if one of the following is true:

  - SUA or the username and password are not configured on the Easy VPN hardware client.
  - IAU is enabled.

  HTTP redirection is automatic and does not require configuration on the Easy VPN Server.

- Preshared keys, digital certificates, tokens and no authentication

  The ASA 5505 supports preshared keys, token-based (e.g., SDI one-time passwords), and "no user authentication" for user authentication. **NOTE**: The Cisco Easy VPN server can use the digital certificate as part of user authorization. See "Enrolling for Digital Certificates" on page 1-1 for instructions.

Group Policy and User Attributes Pushed to the Client

Upon tunnel establishment, the Easy VPN server pushes the values of the group policy or user attributes stored in its configuration to the Easy VPN hardware client. Therefore, to change certain attributes used by the Easy VPN hardware client, you must modify them on the security appliances configured as the primary and secondary Easy VPN servers. This section identifies the group policy attributes pushed to the Easy VPN hardware client.

Note This section serves only as a reference. For instructions on configuring group policies, see "Configuring Group Policies" on page 2-1.

Use Table 34-2 as a guide for determining the group policy attributes to modify on the Easy VPN servers.

Table 12-1 Group Policy and User Attributes Pushed to the Cisco ASA 5505 Configured as an EasyVPN Hardware Client

ASDM Group Policy Tab	Attribute	Description
General	Tunneling Protocols	Specifies the permitted tunneling protocols.
General	Filter	Applies a filter to VPN traffic.
General	Access Hours	Restricts VPN access hours.
General	Simultaneous Logins	Specifies the maximum number of simultaneous logins.
General	Maximum Connect Time	Specifies the maximum number of minutes for VPN connections.
General	Idle Timeout	Specifies the number of minutes a session can be idle before it times out.
General	DNS Servers	Specifies the IP address of the primary and secondary DNS servers, or prohibits the use of DNS servers.
General	WINS Servers	Specifies the IP address of the primary and secondary WINS servers, or prohibits the use of WINS servers.
General	DHCP Scope	Specifies the IP subnetwork to which the DHCP server assigns address to users within this group.
IPSec	Re-authentication on IKE Re-key	Requires XAUTH authentication when IKE rekeys. **Note**: Disable re-xauth if secure unit authentication is enabled.
IPSec	Perfect Forward Security	Commands the VPN client to use perfect forward secrecy.
IPSec	Tunnel Group Lock	Specifies a tunnel group to ensure that users connect to that group.
IPSec	Client Access Rules	Applies access rules.
Client Configuration > General Client Parameters	Banner	Sends a banner to the client after establishing a tunnel.
Client Configuration > General Client Parameters	Default Domain	Sends a domain name to the client.
Client Configuration > General Client Parameters	Split Tunnel DNS Names	Pushes a list of domains for name resolution.

Table 12-1 Group Policy and User Attributes Pushed to the Cisco ASA 5505 Configured as an EasyVPN Hardware Client (continued)

ASDM Group Policy Tab	Attribute	Description
Client Configuration > General Client Parameters	Split Tunnel Policy	Lets a remote-access IPSec client conditionally direct packets over an IPSec tunnel in encrypted form, or to a network interface in cleartext form. Options include the following: • split-tunnel-policy—Indicates that you are setting rules for tunneling traffic. • excludespecified—Defines a list of networks to which traffic goes in the clear. • tunnelall—Specifies that no traffic goes in the clear or to any other destination than the Easy VPN server. Remote users reach Internet networks through the corporate network and do not have access to local networks. • tunnelspecified—Tunnels all traffic from or to the specified networks. This option enables split tunneling. It lets you create a network list of addresses to tunnel. Data to all other addresses travels in the clear, and is routed by the remote user's internet service provider.
Client Configuration > General Client Parameters	Split Tunnel Network List	Specifies one of the following: • No access list exists for split tunneling. All traffic travels across the tunnel. • Identifies the access list the security appliance uses to distinguish networks that require tunneling and those that do not. Split tunneling lets a remote-access IPSec client conditionally direct packets over an IPSec tunnel in encrypted form, or to a network interface in cleartext form. With split-tunneling enabled, 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.
Client Configuration > Cisco Client Parameters	Store Password on Client System	Lets the VPN user save a password in the user profile.
Client Configuration > Cisco Client Parameters	IPSec over UDP	Uses UDP encapsulation for the IPSec tunnels.
Client Configuration > Cisco Client Parameters	IPSec over UDP Port	Specifies the port number for IPSec over UDP.
Client Configuration > Cisco Client Parameters	IPSec Backup Servers	Sets up backup servers on the client in case the primary server fails to respond.
Client Firewall	(All on this tab)	Sets up the firewall parameters on the VPN client.
Hardware Client	Require Interactive Client Authentication	Enables secure unit authentication for VPN hardware clients.
Hardware Client	Require Individual User Authentication	Enables individual user authentication for hardware-based VPN clients.
Hardware Client	Allow Network Extension Mode	Enables or disables network extension mode.

Note IPSec NAT-T connections are the only IPSec connection types supported on the home VLAN of a Cisco ASA 5505. IPSec over TCP and native IPSec connections are not supported.

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

X