Performing Selected User Management Tasks

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

This chapter describes the following user management tasks:

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

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

Configuring Split Tunneling and Network Lists

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

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

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

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

Overview of Configuration Procedure

You configure split tunneling as follows:

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

The instructions in this section refer to the following scenario:

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

For example,

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

Defining a Network List

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

Using CLI Commands

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

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

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

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

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

Using ASDM

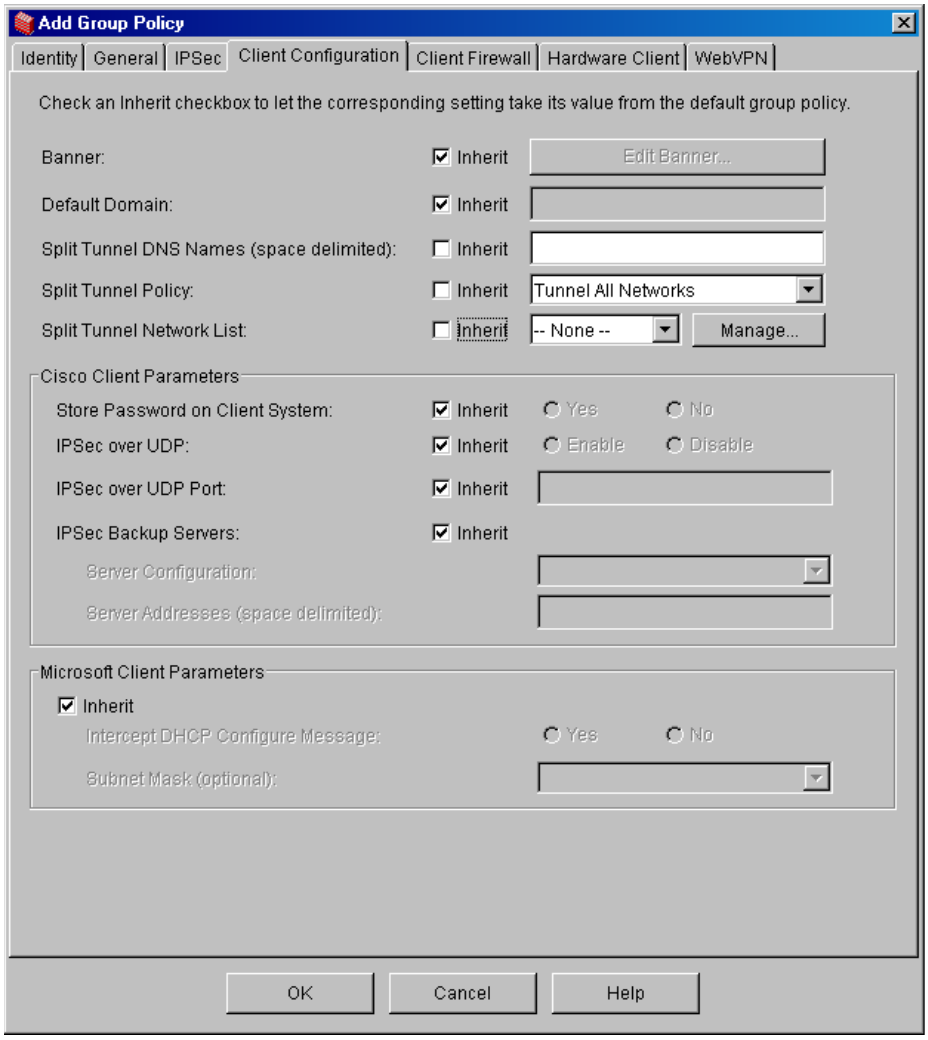
This section shows how to configure network lists for split tunneling using ASDM. In ASDM, you define network lists and other split tunneling parameters under the **Group Policy** panel.

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

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

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

Figure 5-1 Adding a Group Policy—Client Configuration



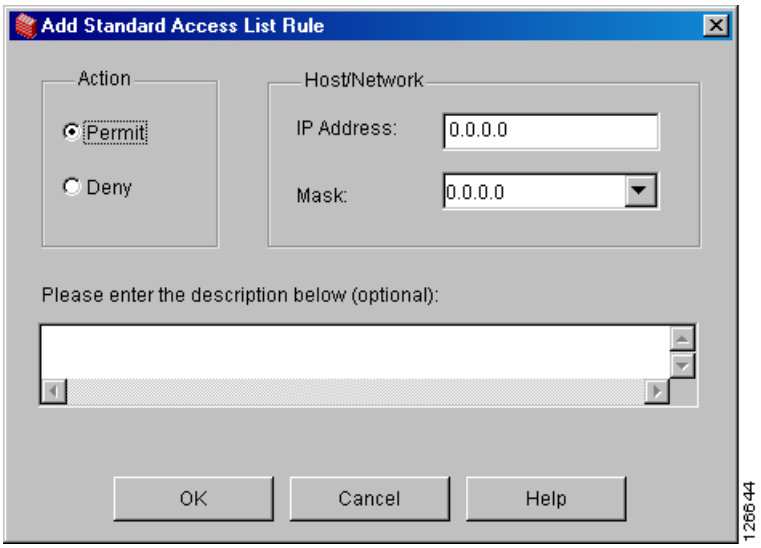
Step 3 To start defining a network list, click to uncheck the **Inherit** box next to **Split Tunnel Network List**.

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

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

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

Figure 5-2 Add an ACL for Split Tunneling



Step 7 Configure the options as follows:

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

Creating a Split Tunneling Group Policy

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

Using CLI Commands

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

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

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

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

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

Using ASDM

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

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

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

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

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

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

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

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

Configuring a Tunnel Group for Split Tunneling

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

Using CLI Commands

Create a tunneling group for split tunneling as follows:

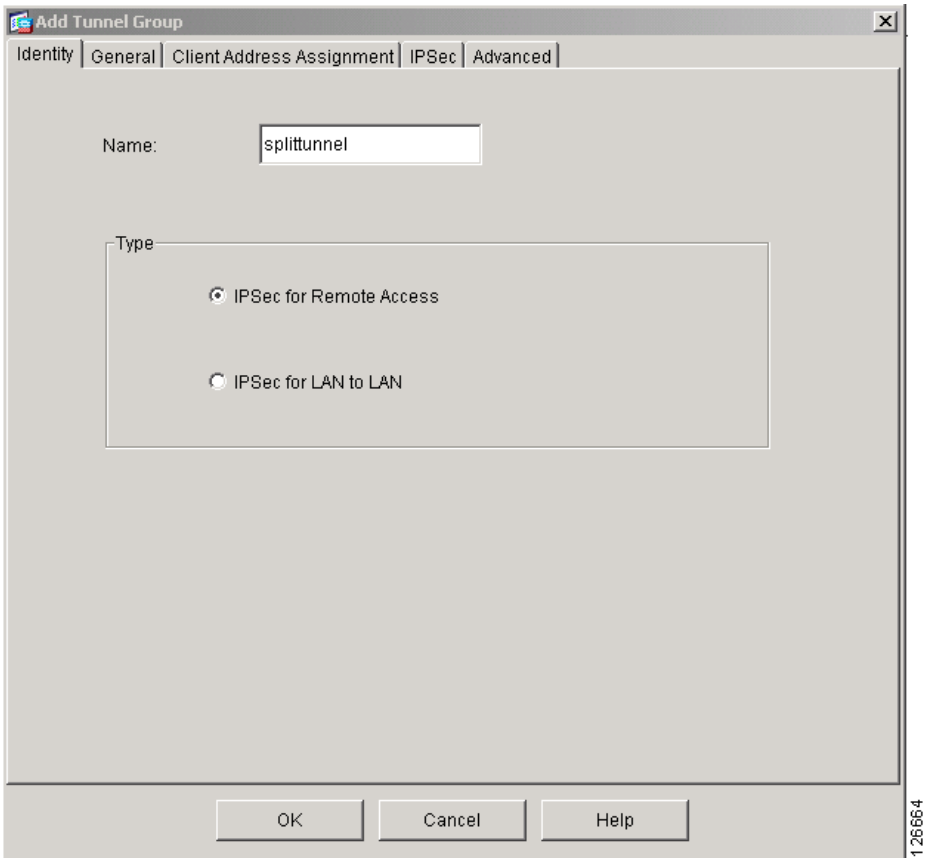
```
hostname(config)# tunnel-group splittunnel type ipsec_ra
hostname(config)# tunnel-group splittunnel general-attributes
hostname(config-general)# default-group-policy splitgroup
hostname(config)# tunnel-group splittunnel ipsec-attributes
hostname(config-ipsec)# pre-shared-key v$bx8*c
```

Using ASDM

Create a tunneling group for split tunneling as follows:

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

Figure 5-3 Adding a Tunnel Group—Identity tab



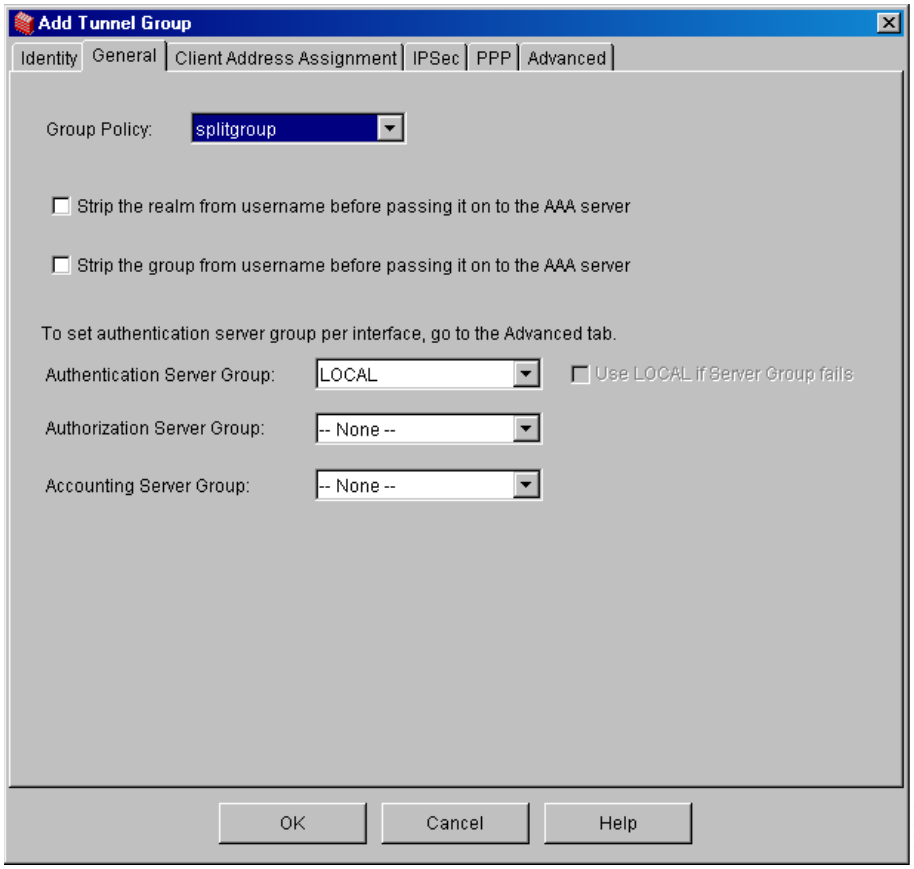
Step 2 Type the name for the tunnel group in the **Name** box.

For this example, the name is splittunnel.

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

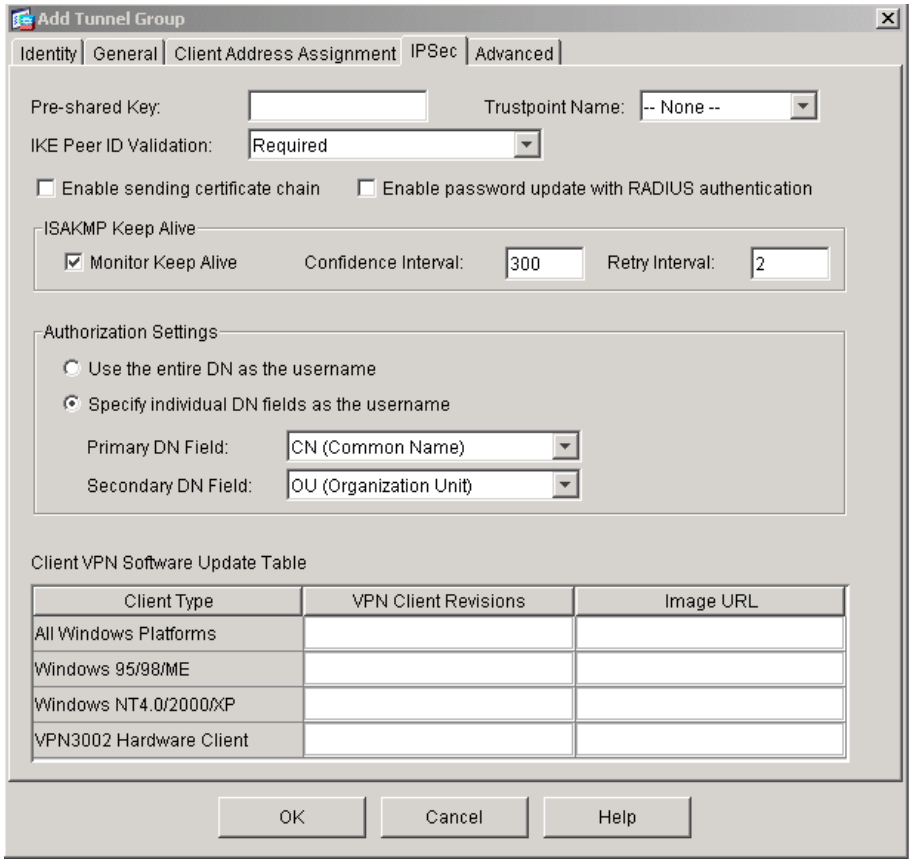
Step 4 Click the **General** tab and select the group policy from the **Group Policy** list. For this example, click **splitgroup**, the group policy configured in the previous section (see Figure 5-4).

Figure 5-4 Adding Tunnel Group—General tab



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

Figure 5-5 Adding a Tunnel Group—IPSec Tab



Split DNS Names

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

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

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

Configuring a Client Firewall and VPN

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

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

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

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

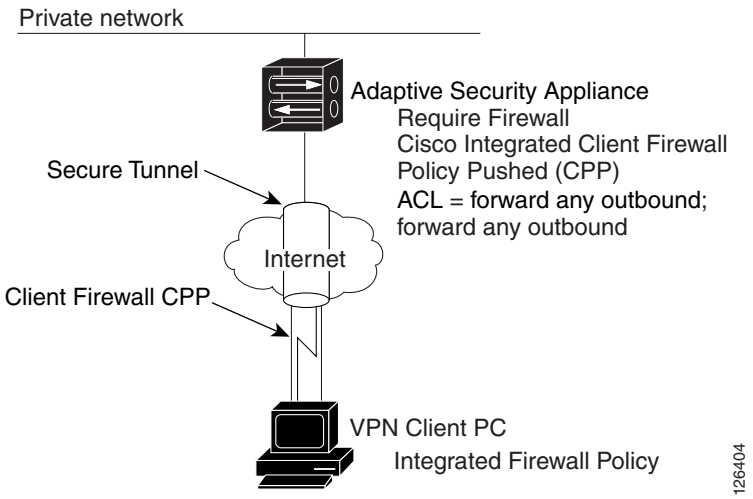
In the second option, you might prefer to enforce a centralized firewall policy for personal firewalls on VPN client PCs. A common example would be to block Internet traffic to remote PCs in a tunnel group using split tunneling. This approach protects the PCs, and therefore the central site, from intrusions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

Configuring a Client Firewall to Use as a Default

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

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

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



Configuring Access Lists for a Client Firewall Configuration (CLI)

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

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

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

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

Configuring a Client Firewall in a Group Policy

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

Using CLI Commands

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

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

group-policy *name* **attributes**

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

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

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

Using ASDM

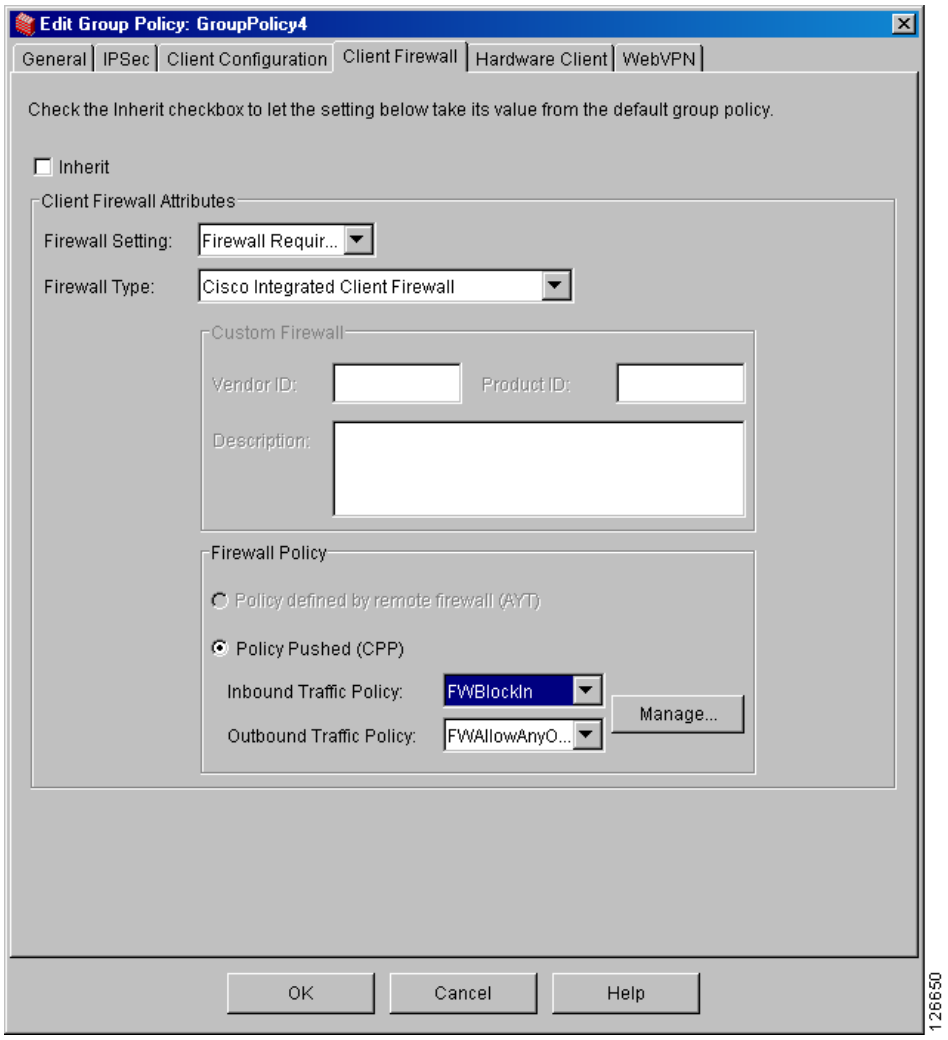
To configure client firewall protection using ASDM, add a group policy or edit an existing one. This example edits an existing policy named GroupPolicy4.

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

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

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

Figure 5-7 Client Firewall Options



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

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

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

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

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

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

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

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

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

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

Click one of the following:

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

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

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

Table 5-1 Firewall Policy Options Available for Each Firewall

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

Table 5-1 Firewall Policy Options Available for Each Firewall

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

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

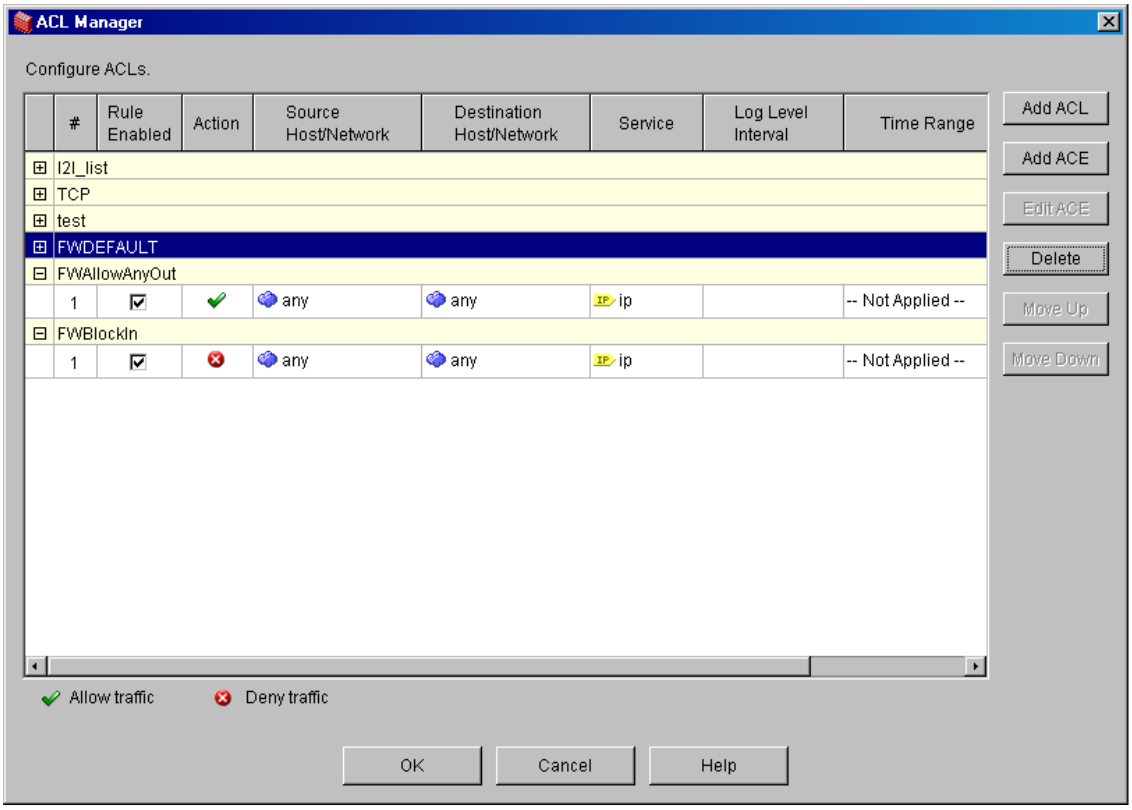
This example specifies **Policy Pushed (CPP)**. The **Firewall Policy** list contains the following options:

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

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

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

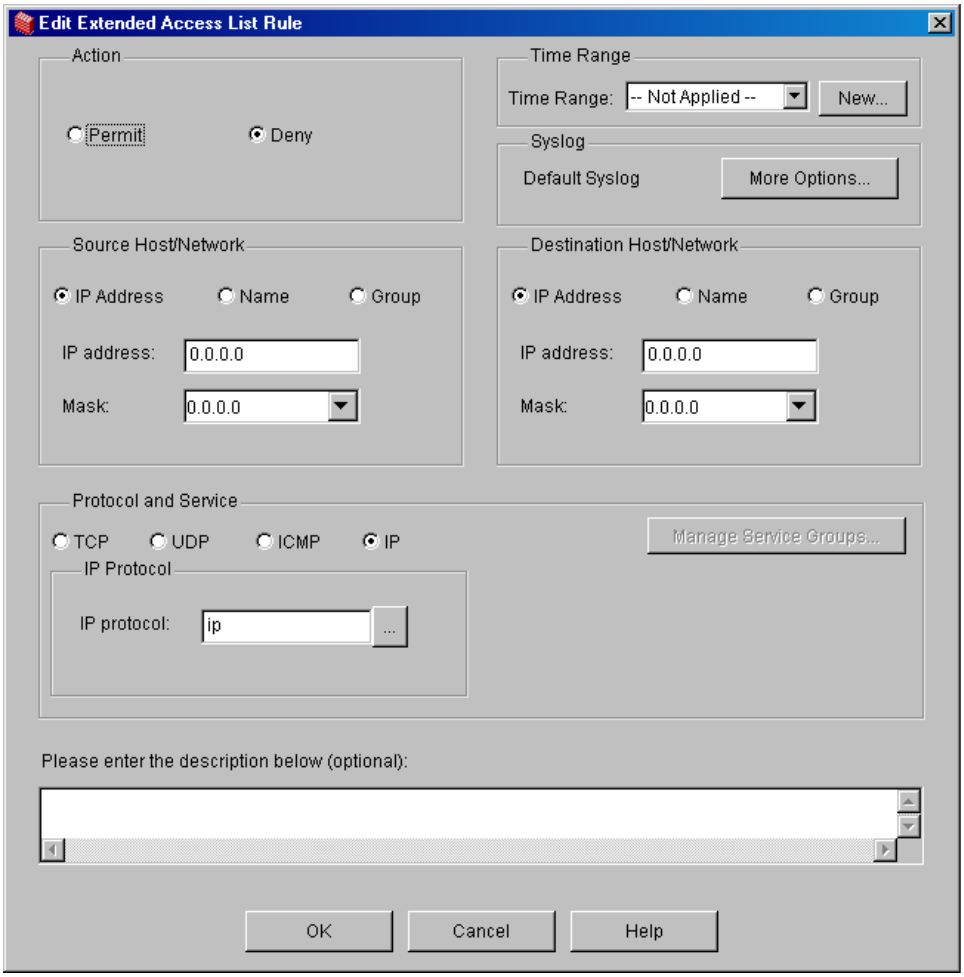
Figure 5-8 Using the ACL Manager



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

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

Figure 5-9 Adding an Access List Rule



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

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

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

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

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

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

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

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

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

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

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

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

Configuring a Client Firewall to Allow HTTP Traffic

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

Using CLI Commands

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

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

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

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

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

Using ASDM

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

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

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

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

b. Accept the default **internal**.

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

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

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

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

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

Step 6 Click **Manage**.

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

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

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

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

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

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

e. Click **OK**.

Step 9 Click **OK**.

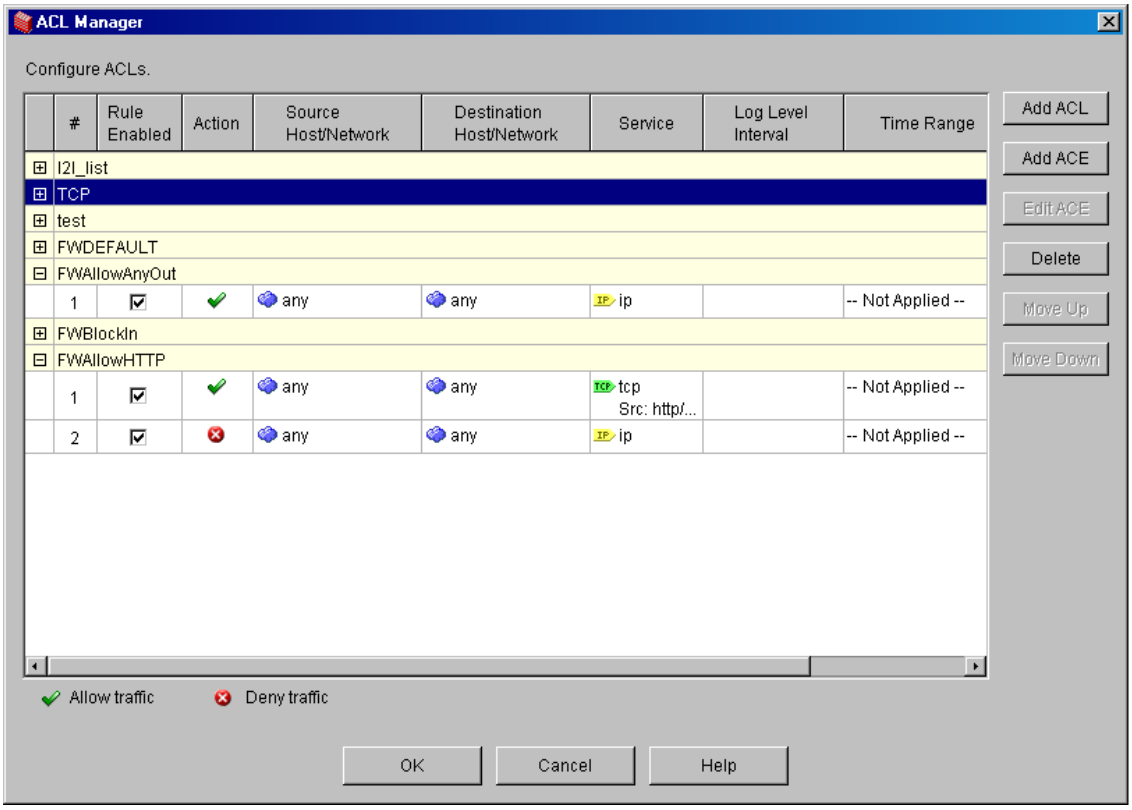
Step 10 On the **Client Firewall** tab, under **Firewall Policy** and **Policy Pushed (CPP)**, click **FWAllowHTTP** in the **Inbound Traffic Policy** list and click **FWAllowAnyOut** in the **Outbound Traffic Policy** list. Then click **Manage**.

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

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

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

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



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

Authenticating with External Servers

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

Overview of Configuration Procedure

To configure external authentication, use the following procedure:

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

This example uses the following scenario:

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

Creating an IP Address Pool

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

Using CLI Commands

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

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

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

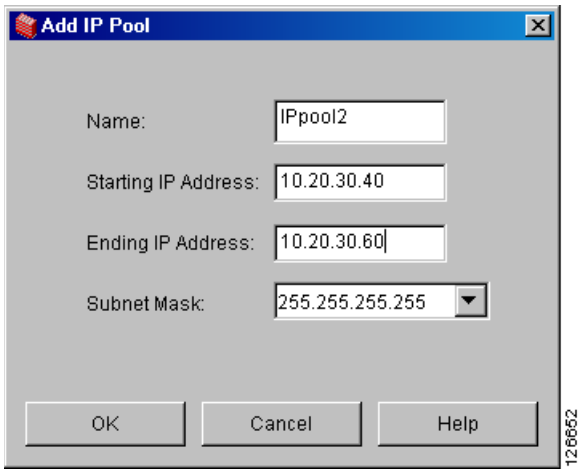
```
hostname(config)# ip local pool IPPool2 10.20.30.40-10.20.30.60
hostname(config)#
```

Using ASDM

To create an IP address pool:

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

Figure 5-11 Adding an IP Address Pool



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

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

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

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

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

Adding a Server Group

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

- RADIUS protocol
- Single accounting mode
- Timed reactivation mode

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

  The default value is 3.

Using CLI Commands

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

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

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

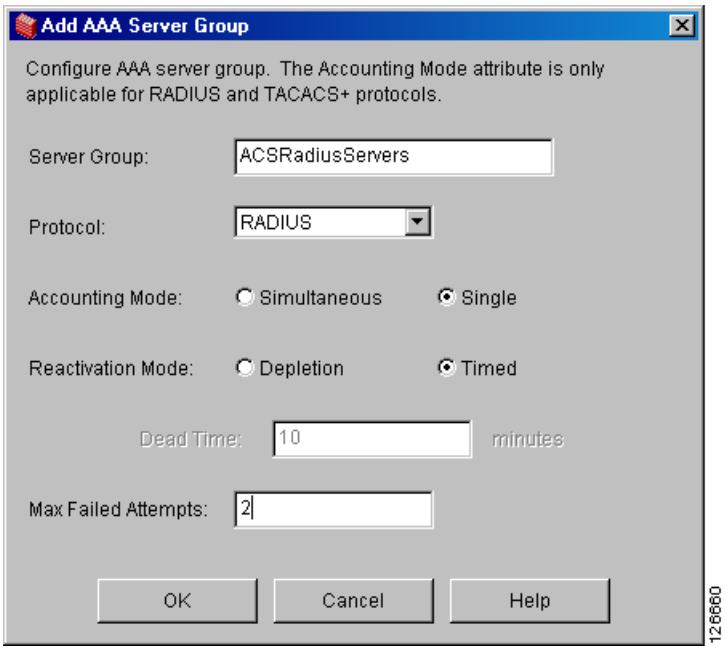
The following commands configure a AAA server group named RadiusServer that uses the RADIUS protocol.

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

Using ASDM

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

Figure 5-12 Adding an AAA Server Group



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

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

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

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

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

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

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

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

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

Adding a AAA Hosts to the AAA Server Group

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

Using CLI Commands

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

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

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

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

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

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

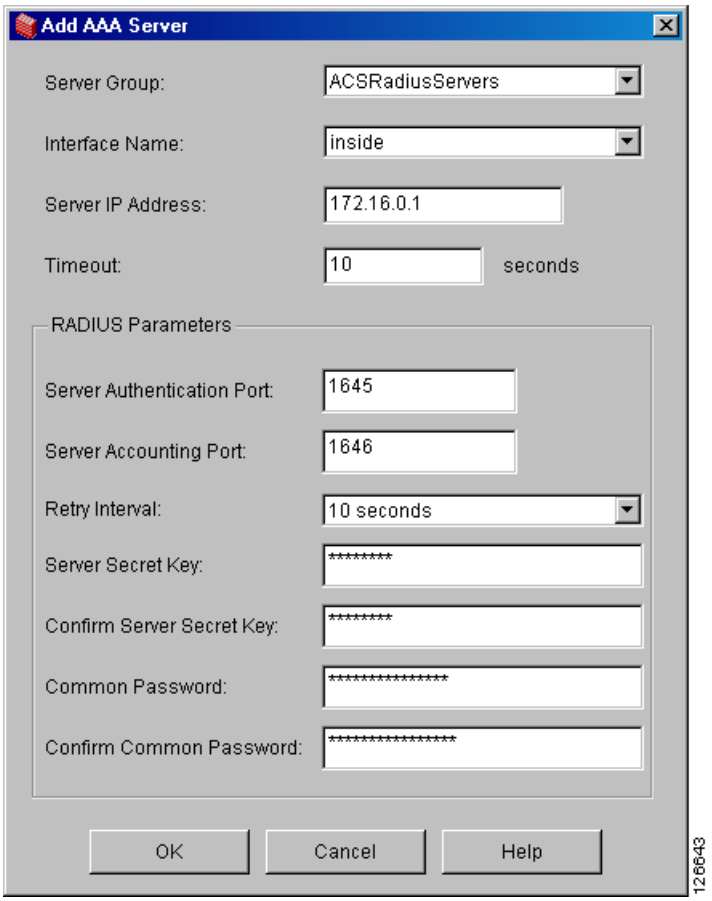
```
hostname(config-aaa-server-group)# retry-interval 5
hostname(config-aaa-server-group)# timeout 16
hostname(config-aaa-server-group)# key x5*zbrct
hostname(config-aaa-server-group)#
hostname(config)# aaa-server ACSRadiusServers (inside) host 172.16.0.2
hostname(config-aaa-server-group)# retry-interval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

Using ASDM

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

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

Figure 5-13 Adding an AAA Server for External Authentication



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

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

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

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

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

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

Note Only RADIUS servers use a common password.

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

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

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

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

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

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

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

Adding a Tunnel Group for Remote Access Using External Authentication

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

Using CLI Commands

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

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

Using ASDM

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

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

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

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

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