



## 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, page 12-1](#)
- [Getting Started \(Easy VPN Hardware Client Only\), page 12-2](#)
- [Configuring Basic Settings, page 12-3](#)
- [Configuring Advanced Settings, page 12-9](#)
- [Guidelines for Configuring the Easy VPN Server, page 12-13](#)

## Comparing Tunneling Options

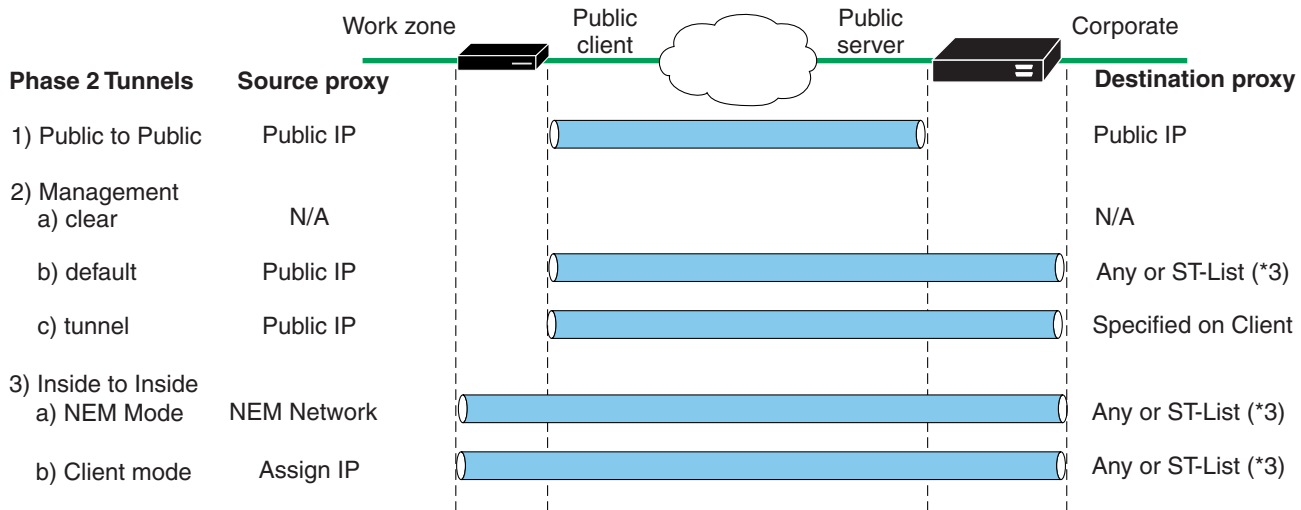
The tunnel types the Cisco ASA 5505 configured as an Easy VPN hardware client sets up depends on a combination of the following factors:

- 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



Configuration factors:

1. Certs or Preshare Keys (Phase 1- main mode or aggressive mode)
2. Mode: Client or NEM
3. All-or-nothing or Split-tunneling
4. Management Tunnels
5. IUA to VPN3000 or ASA headend

\* Only for ASA or VPN3000 Headends

153780

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](#).

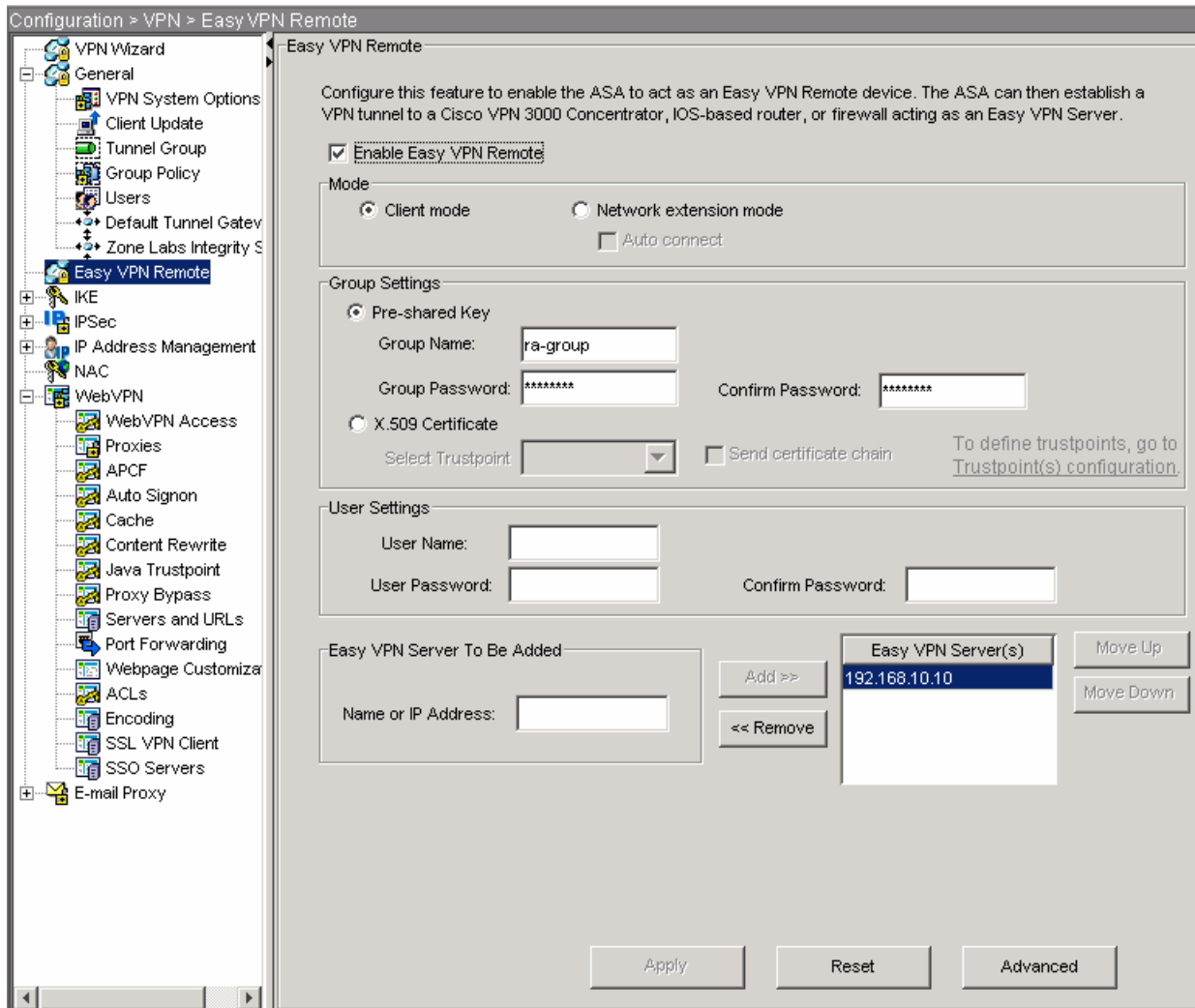
- (Optional) Retrieve the username and password from the server for the Easy VPN hardware client to use in response to an IKE Extended Authenticate (Xauth) challenge from the server.
- IP addresses of the primary and backup headends that will take the role of the Easy VPN servers.

## 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

**Advanced Easy VPN Properties**

**MAC Exemption**  
Configure the MAC Addresses/Masks of devices that need to be exempted from authentication, configured on the Firewall for an Easy VPN Remote Connection.

MAC Address:  Add >>

MAC Mask:  << Remove

MAC Address/Mask

---

**Tunneled Management**  
Specify/Clear the IP Addresses/Masks of the remote network(s), managing the Easy VPN Remote Client's public/internet interface over the tunnel

Enable Tunneled Management  Clear Tunneled Management

IP Address:  Add >>

Mask:  << Remove

IP Address/Mask

---

**IPSec Over TCP**

Enable Enter port Number:

---

**Server Certificate**

Server Certificate:  To define certificate maps, go to Configuration > VPN > IKE > Certificate Group Matching > Rules.

OK Cancel Help

153075

**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. <b>Note:</b> 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: <ul style="list-style-type: none"> <li>split-tunnel-policy—Indicates that you are setting rules for tunneling traffic.</li> <li>excludespecified—Defines a list of networks to which traffic goes in the clear.</li> <li>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.</li> <li>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.</li> </ul>
Client Configuration > General Client Parameters	Split Tunnel Network List	Specifies one of the following: <ul style="list-style-type: none"> <li>No access list exists for split tunneling. All traffic travels across the tunnel.</li> <li>Identifies the access list the security appliance uses to distinguish networks that require tunneling and those that do not.</li> </ul> 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.

---

