

## Scenario: Easy VPN Hardware Client Configuration

---

This chapter describes how to configure the ASA 5505 to function as an Easy VPN hardware client. The ASA 5505 can be used as part of an Easy VPN deployment consisting of multiple devices that make up a Virtual Private Network (VPN).

This chapter includes the following sections:

- [Using an ASA 5505 as an Easy VPN Hardware Client, page 11-1](#)
- [Client Mode and Network Extension Mode, page 11-3](#)
- [Configuring the Easy VPN Hardware Client, page 11-5](#)
- [Configuring Advanced Easy VPN Attributes, page 11-11](#)
- [What to Do Next, page 11-12](#)

## Using an ASA 5505 as an Easy VPN Hardware Client

A Cisco Easy VPN hardware client (sometimes called an “Easy VPN remote device”) enables companies with multiple sites to establish secure communications among them and share resources. A Cisco Easy VPN solution consists of an Easy VPN server at the main site and Easy VPN hardware clients at the remote offices.

The Cisco ASA 5505 can function as a Cisco Easy VPN hardware client or as a Cisco Easy VPN server (sometimes called a “headend device”), but not both at the same time.

Using an Easy VPN solution simplifies the deployment and management of a VPN in the following ways:

- Hosts at remote sites no longer have to run VPN client software.
- Security policies reside on a central server and are pushed to the remote hardware clients when a VPN connection is established.
- Few configuration parameters need to be set locally, minimizing the need for on-site administration.

Figure 11-1 illustrates how Easy VPN components can be deployed to create a VPN.

**Figure 11-1** *Easy VPN Components in a Virtual Private Network*



When used as an Easy VPN hardware client, the ASA 5505 can also be configured to perform basic firewall services, such as protecting devices in a DMZ from unauthorized access. However, if the ASA 5505 is configured to function as an Easy VPN hardware client, it cannot establish other types of tunnels. For example, the ASA 5505 cannot function simultaneously as an Easy VPN hardware client and as one end of a standard peer-to-peer VPN deployment.



**Note**

---

Load balancing is supported with VPN remote sessions that are initiated with the ASA 5505 when it is acting as an Easy VPN client.

---

# Client Mode and Network Extension Mode

The Easy VPN hardware client supports one of two modes of operation: Client Mode or Network Extension Mode (NEM). The mode of operation determines whether the hosts behind the Easy VPN hardware client are accessible from the enterprise network over the tunnel.

Client Mode, also called Port Address Translation (PAT) mode, isolates all devices on the Easy VPN client private network from those on the enterprise network. The Easy VPN client performs PAT for all VPN traffic for its inside hosts. IP address management is neither required for the Easy VPN client inside interface or the inside hosts.

NEM makes the inside interface and all inside hosts routable across the enterprise network over the tunnel. Hosts on the inside network obtain their IP addresses from an accessible subnet (statically or with DHCP) that is preconfigured 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 ASA 5505 configured for NEM mode supports automatic tunnel initiation. The configuration must store the group name, username, and password.

Automatic tunnel initiation is disabled if secure unit authentication is enabled. The network and addresses on the private side of the Easy VPN client are hidden, and cannot be accessed directly.

The Easy VPN hardware client does not have a default mode. However, if you do not specify the mode in ASDM, ASDM automatically selects client mode. When you configure the Easy VPN hardware client using the CLI, you must specify a mode.

[Figure 11-2](#) shows a sample network topology with the ASA 5505 running in Easy VPN Client Mode. When configured in Client Mode, devices on the inside interface of the ASA 5505 cannot be accessed by devices behind the Easy VPN server.

**Figure 11-2**      *Topology with ASA 5505 in Client Mode*



When configured in Network Extension Mode, the ASA 5505 does not hide the IP addresses of local hosts by substituting a public IP address. Therefore, hosts on the other side of the VPN connection can communicate directly with hosts on the local network.

When configuring NEM, the network behind the Easy VPN client should not overlap the network behind the Easy VPN server.

[Figure 11-3](#) shows a sample network topology with the ASA 5505 running in Network Extension Mode.

**Figure 11-3**      *Network Topology with ASA 5505 Running in Network Extension Mode*



Use the following guidelines when deciding whether to configure the ASA 5505 in Client Mode or Network Extension Mode.

Use Client Mode if:

- You want VPN connections to be initiated when a device behind the Easy VPN hardware client attempts to access a device on the enterprise network.
- You do not want devices behind the Easy VPN hardware client to be accessible by devices on the enterprise network.

Use Network Extension Mode if:

- You want VPN connections to be established automatically and to remain open even when not required for transmitting traffic.
- You want remote devices to be able to access hosts behind the Easy VPN hardware client.

## Configuring the Easy VPN Hardware Client

The Easy VPN server controls the security policies enforced on the ASA 5505 Easy VPN hardware client. However, to establish the initial connection to the Easy VPN server, you must complete some configuration locally.

You can perform this configuration procedure by using ASDM or by using the command-line interface.

This section includes the following topics:

- [Starting ASDM With the ASDM Launcher, page 11-6](#)
- [Configuring the Hardware Client, page 11-9](#)

## Starting ASDM With the ASDM Launcher

This section describes how to start ASDM using the ASDM Launcher software. If you have not installed the ASDM Launcher software, see [Installing the ASDM Launcher, page 5-5](#). If you prefer to access ASDM directly with a web browser or using Java, see [Starting ASDM with a Web Browser, page 5-8](#).

To start ASDM, perform the following steps:

- 
- Step 1** From your desktop, double-click the Cisco ASDM Launcher icon.  
The Cisco ASDM-IDM Launcher dialog box appears.



- Step 2** Enter the IP address or the device name of the adaptive security appliance.
- Step 3** Leave the Username and Password fields blank.



---

**Note** By default, no Username and Password are set for the Cisco ASDM-IDM Launcher.

---

**Step 4** Click **OK**.

**Step 5** Click **Yes** to accept the certificates.

The adaptive security appliance checks to see if updated software is available and if so, downloads it automatically.

**Step 6** Click **Yes** to all subsequent authentication and certificate dialog boxes.

The ASDM main window appears.

■ Configuring the Easy VPN Hardware Client



## Configuring the Hardware Client

To configure the ASA 5505 to act as an Easy VPN hardware client, perform the following steps:

- 
- Step 1** In the ASDM main window, choose **Configuration > Remote Access VPN > Easy VPN Remote**.

The Easy VPN Remote pane appears.



- Step 2** Check the **Enable Easy VPN Remote** check box to enable Easy VPN on the device. If you uncheck it, when you apply the configuration changes, you are prompted to specify if you want to clear the entire Easy VPN configuration or whether you want to disable the Easy VPN client temporarily.



---

**Note** When Easy VPN Remote is enabled, you cannot make any configuration changes to IPsec rules, tunnel policy, IKE, or SSL VPN settings.

---

- Step 3** In the Mode area, to specify which mode the Easy VPN remote hardware client should run in, click the **Client Mode** or **Network Extension Mode** radio button.
- Step 4** To have the Easy VPN remote hardware client automatically run in Network Extension Mode, check the **Auto Connect** check box.
- Step 5** In the Group Settings area, specify the type of authentication that the VPN devices should use by choosing one of the following options.
- To use a pre-shared key for authentication, click the **Pre shared key** radio button and enter a Group Name and Group Password.
  - To use an X.509 certificate for authentication, click the **X.509 Certificate** radio button. Choose the certificate from the drop-down list, check the **Send certificate chain** check box, and click the **Identity Certificates** link to open the Certificate Management pane, from which you can configure and manage certificates. For more information about managing certificates, see the ASDM online help.
- Step 6** In the User Settings area, specify the User Name and User Password to be used by the ASA 5505 when establishing a VPN connection.
- Step 7** Specify one or more Easy VPN servers from which this device obtains VPN security policies.
- a. In the Easy VPN server To Be Added area, enter the hostname or IP address of an Easy VPN server. You must add at least one Easy VPN server.
  - b. Click **Add** or **Remove** to add or remove servers from the Easy VPN servers list. The first server on the list is used as the primary server. Other servers on the list provide redundancy. To change the order of the list, click **Move Up** or **Move Down**. You can specify up to nine backup servers, for a total of ten servers.
- Step 8** Click **Apply** to push the configuration to the adaptive security appliance.
- Step 9** To save the configuration, click **Save** on the toolbar.
-

# Configuring Advanced Easy VPN Attributes

You might need to perform some advanced configuration tasks if your network meets any of the following conditions:

- Your network includes devices that cannot perform authentication, and therefore cannot participate in individual unit authentication. Such devices include Cisco IP Phones, printers, and the like.

To accommodate these devices, you can enable the device pass-through feature.

- Your ASA 5505 is operating behind a NAT device.

In this case, you must use tunneled management attributes to specify whether device management should occur in the clear or through the tunnel and the network or networks are allowed to manage the Easy VPN connection through the tunnel.



---

**Note**

When behind a NAT device, the public address of the ASA 5505 is not accessible unless you add static NAT mappings on the NAT device.

---

To configure these attributes, click **Advanced** in the Easy VPN Remote configuration pane to open the Advanced Easy VPN Properties pane. For specific information about configuration settings for this pane, see the ASDM online help.

## What to Do Next

If you are deploying the adaptive security appliance only as an Easy VPN hardware client, you have completed the initial configuration. You may want to consider performing some of the following additional steps:

<b>To Do This...</b>	<b>See...</b>
Refine configuration and configure optional and advanced features	<i>Cisco Security Appliance Command Line Configuration Guide</i>
Learn about daily operations	<i>Cisco Security Appliance Command Reference</i> <i>Cisco Security Appliance System Log Messages Guide</i>