

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 9-1](#)
- [Client Mode and Network Extension Mode, page 9-3](#)
- [Configuring the Easy VPN Hardware Client, page 9-5](#)
- [What to Do Next, page 9-9](#)

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 9-1 illustrates how Easy VPN components can be deployed to create a VPN.

Figure 9-1 *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.

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 9-2](#) 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 9-2 *Topology with ASA 5505 in Client Mode*



When configured in Easy VPN 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 your the network behind the Easy VPN server

[Figure 9-3](#) shows a sample network topology with the ASA 5505 running in Network Extension Mode.

Figure 9-3 **Network Topology with ASA 5505 Running in Network Extension Mode**



Use the following guidelines when deciding whether to configure the ASA 5505 in Easy VPN 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 describes how to perform the configuration using ASDM.

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

-
- Step 1** At a PC that has access to the inside interface of the ASA 5505, start ASDM.
- a. Start a web browser.
 - b. In the address field of the browser, enter the factory default IP address in the address field: **https://192.168.1.1/**.
-  **Note** Remember to add the “s” in “**https**” or the connection fails. HTTPS (HTTP over SSL) provides a secure connection between your browser and the adaptive security appliance.
-
- c. In the window that requires you to choose the method you want to use to run the ASDM software, choose either to download the ASDM Launcher or to run the ASDM software as a Java applet.
- Step 2** In the ASDM window, click the **Configuration** tool.
- Step 3** Click the **VPN** tool, and then check the Enable **Easy VPN Remote** check box.

If you check the **Enable Easy VPN Remote** check box, Easy VPN is enabled on the device when you click Apply. 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 just want to disable the Easy VPN client temporarily.

The Easy VPN Remote configuration pane appears.



- Step 4** Check the **Enable Easy VPN Remote** check box.
- Step 5** To specify which mode the Easy VPN remote hardware client should run in, click **Client Mode** or **Network Extension Mode** radio button.
- Step 6** In the Group Settings area, specify the type of authentication the VPN devices should use.
- To specify that the VPN devices should use a text password for authentication, click the **Group Password** radio button and enter a Group Name and Group Password.
- Step 7** 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 8** Specify one or more Easy VPN servers from which this device obtains VPN security policies.
- In the Easy VPN server To Be Added area, enter the hostname or IP address of an Easy VPN server.
 - 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. If you are using a Cisco VPN 3000 series concentrator as the headend device, the concentrator can be configured to balance the load across all servers in the list.

You can specify up to nine backup servers, for a total of ten servers.

- Step 9** Click **Apply** to push the configuration to the adaptive security appliance. To save the configuration, click the **Save** button on the top 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 are incapable of performing authentication, and therefore are incapable of participating 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 allowed to manage the Easy VPN connection through the tunnel.



Note The public address of the ASA 5505 is not accessible when behind the NAT device unless you add static NAT mappings on the NAT device.

To configure these attributes, click **Advanced** in the Easy VPN Remote configuration pane. See the online help for specific information about configuration settings.

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:

To Do This...	See...
Configure the ASA 5505 to protect a DMZ web server	Chapter 6, “Scenario: DMZ Configuration”
Refine configuration and configure optional and advanced features	Cisco Security Appliance Command Line Configuration Guide
Learn about daily operations	Cisco Security Appliance Command Reference Cisco Security Appliance Logging Configuration and System Log Messages

■ What to Do Next