

Easy VPN

This chapter describes how to configure any ASA as an Easy VPN Server, and the ASA with FirePOWER-5506-X, 5506W-X, 5506H-X, and 5508-X models as an Easy VPN Remote hardware client.

- About Easy VPN, on page 1
- Configure Easy VPN Remote, on page 4
- Configure Easy VPN Server, on page 7
- Feature History for Easy VPN, on page 8

About Easy VPN

Cisco Ezvpn greatly simplifies configuration and deployment of VPN for remote offices and mobile workers. Cisco Easy VPN offers flexibility, scalability, and ease of use for site-to-site and remote-access VPNs. It implements the Cisco Unity Client protocol, allowing administrators to define most VPN parameters on the Easy VPN Server, simplifying the Easy VPN Remote configuration.

The Cisco ASA with FirePOWER models 5506-X, 5506W-X, 5506H-X, and 5508-X support Easy VPN Remote as a hardware client that initiates the VPN tunnel to an Easy VPN Server. The Easy VPN server can be another ASA (any model), or a Cisco IOS-based router. An ASA cannot function as both an Easy VPN Remote and an Easy VPN Server simultaneously.

Note The Cisco ASA 5506-X, 5506W-X, 5506H-X and 5508-X models support L3 switching not L2 switching. Use an external switch when using Easy VPN Remote with multiple hosts or devices on the inside network. A switch is not required if a single host is on the inside network of the ASA.

The following sections describe Easy VPN options and settings.

Easy VPN Interfaces

Upon system startup, the Easy VPN external and internal interfaces are determined by their security level. The physical interface with the lowest security level is used for the external connection to an Easy VPN server. The physical or virtual interface with the highest security level is used for the internal connection to secure resources. If Easy VPN determines that there are two or more interfaces with the same highest security level, Easy VPN is disabled.

You can change the internal secure interface using the **vpnclient secure interface** command if desired, to or from, a physical or virtual interface. You cannot change the external interface from the automatically selected default, physical interface.

For example, on an ASA5506 platform, the factory configuration has a BVI with the highest security level interface set to 100 (with its member interfaces also at level 100), and an external interface with security level zero. By default, Easy VPN selects these interfaces.

When a virtual interface (a Bridged Virtual Interface or BVI) is selected upon startup or assigned by the administrator as the internal secure interface, the following applies:

- All BVI member interfaces are considered Internal Secured interfaces irrespective of their own security levels.
- ACL and NAT rules need to be added on all the member interfaces. AAA rules are added on the BVI interface alone.

Easy VPN Connections

Easy VPN uses IPsec IKEv1 tunnels. The Easy VPN Remote hardware client's configuration must be compatible with the VPN configuration on the Easy VPN Server headend. If using secondary servers, their configuration must be identical to the primary server.

The ASA Easy VPN Remote configures the IP address of the primary Easy VPN Server and optionally, up to 10 secondary (backup) servers. Use the **vpnclient server** command in global configuration mode to configure these servers. If unable to set up the tunnel to the primary server, the client tries the connection to the first secondary VPN server, and then sequentially down the list of VPN servers at 8 second intervals. If the setup tunnel to the first secondary server fails, and the primary server comes online during this time, the client will proceed to set up the tunnel to the second secondary VPN server.

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 IPsec within TCP packets to enable secure tunneling. Use the **vpnclient ipsec-over-tcp** command to configure this. If your environment allows UDP, however, configuring IPsec over TCP adds unnecessary overhead.

Easy VPN Tunnel Groups

Upon tunnel establishment, the Easy VPN Remote specifies the tunnel group, configured on the Easy VPN Server, that will be used for the connection. The Easy VPN Server pushes group policy or user attributes to the Easy VPN Remote hardware client determining tunnel behavior. To change certain attributes, you must modify them on the ASAs configured as primary or secondary Easy VPN Servers.

The Easy VPN Remote client specifies the group policy using the **vpnclient vpngroup** command to configure its name and pre-shared key, or the **vpnclient trustpoint** command to identify a pre-configured trustpoint.

Easy VPN Mode of Operation

The mode determines whether the hosts behind the Easy VPN Remote are accessible or not from the enterprise network over the tunnel:

- Client mode, also called Port Address Translation (PAT) mode, isolates all devices on the Easy VPN Remote private network from those on the enterprise network. The Easy VPN Remote performs Port Address Translation (PAT) for all VPN traffic for its inside hosts. The network and addresses on the

private side of the Easy VPN Remote are hidden, and cannot be accessed directly. IP address management is not required for the Easy VPN Client inside interface or the inside hosts.

- Network Extension Mode (NEM) makes the inside interface and all inside hosts route-able 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 or tunnel for each host on the inside network, the Easy VPN Remote provides tunneling for all of the hosts.

The Easy VPN Server defaults to Client mode. To configure NEM mode use the **nem enable** command in group policy configuration mode. Specifying one of the modes of operation on the Easy VPN Remote is mandatory before establishing a tunnel because it does not have a default mode. On the Easy VPN Remote use the **vpnclient mode** command to configure PAT or NEM.



Note The Easy VPN Remote ASA configured for NEM mode supports automatic tunnel initiation. Automatic initiation requires the configuration and storage of credentials used to set up the tunnel. Automatic tunnel initiation is disabled if secure unit authentication is enabled.

An Easy VPN Remote in Network Extension Mode with multiple interfaces configured builds a tunnel for locally encrypted traffic only from the interface with the highest security level.

Easy VPN User Authentication

The ASA Easy VPN Remote can store the username and password for automatic login using the **vpnclient username** command..

For additional security, the Easy VPN Server can require:

- Secure unit authentication (SUA)—ignores the configured username and password requiring a user to manually authenticate. By default, SUA is disabled, enable SUA on the Easy VPN Serverusing the **secure-unit-authentication enable** command .
- Individual user authentication (IUA)—requires users behind the Easy VPN Remote to authenticate before receiving access to the enterprise VPN network. By default, IUA is disabled, enable IUA on the Easy VPN Serverusing the **user-authentication enable** command .

  When using IUA, specific devices, such as Cisco IP Phones or printers, behind the hardware client will need to bypass individual user authentication. To configure this, specify IP phone bypass, using the **ip-phone-bypass** command, on the Easy VPN Server and MAC address exemption, using the **mac-exempt** command, on the Easy VPN Remote.

  Additionally, the Easy VPN Server can set or remove the idle timeout period after which the Easy VPN Server terminates the client's access using the **user-authentication-idle-timeout** command on the Easy VPN Server.

The Cisco Easy VPN server intercepts HTTP traffic and redirects the user to a login page if the user name and password is not configured, or SUA is disabled, or IUA is enabled. HTTP redirection is automatic and does not require configuration on the Easy VPN Server.

Remote Management

The ASA operating as an Easy VPN Remote hardware client supports management access using SSH or HTTPS, with or without additional IPsec encryption.

By default, management tunnels use IPsec encryption within SSH or HTTPS encryption. You can *clear* the IPsec encryption layer allowing management access outside of the VPN tunnel using the **vpnclient management clear** command. Clearing tunnel management merely removes the IPsec encryption level and does not affect any other encryption, such as SSH or HTTPS, that exists on the connection.

For additional security, the Easy VPN Remote can require the IPsec encryption and limit administrative access to specific hosts or networks on the corporate side using the **vpnclient management tunnel** command in global configuration mode.

Use **no vpnclient management** to return to default remote management operation.



Note Do not configure a management tunnel on a ASA Easy VPN Remote if a NAT device is operating between it and the Internet. In that configuration, clear remote management using the **vpnclient management clear** command.

Regardless of your configuration, DHCP requests (including renew messages) should not flow over IPsec tunnels. Even with a vpnclient management tunnel, DHCP traffic is prohibited.

Configure Easy VPN Remote

Before you begin

Gather the following information to configure the Easy VPN Remote:

- The address of the primary Easy VPN Server, and secondary servers if available.
- The addressing mode, Client or NEM, the Easy VPN Remote should operate in.
- The Easy VPN Server group policy name and password (pre-shared key), or a pre-configured trust point that will select and authenticate the desired group policy.
- The user(s) configured on the Easy VPN Server that are authorized to use the VPN tunnel.
- If a BVI interface is being used for a remote management interface, **management-access** must be configured on that interface.

Procedure

Step 1 Configure the Easy VPN Server addresses.

vpnclient server *ip-primary* [*ip-secondary-1... ip-secondary-n*]

- *ip-primary-address*—the IP address or DNS name of the primary Easy VPN server.
- *ip-secondary-n* (Optional)—a list of the IP addresses or DNS names of up to ten backup Easy VPN servers. Use a space to separate the items in the list.

Example:

```
asa(config)#vpnclient server 10.10.10.15 10.10.10.30 192.168.10.10
```

Step 2 (Optional) Reassign the internal secure interface if the automaticly chosen default one is not desired.

Upon startup, The physical interface or BVI with the highest security level is used for the internal connection to secure resources. If you prefer a different interface, use the **vpnclient secure interface** *interface-name* command. A physical or virtual interface can be assigned.

Step 3 Specify the mode of operation.

vpnclient mode {**client-mode** | **network-extension-mode**}

- **client-mode**—Uses Port Address Translation (PAT) mode to isolate the addresses of the inside hosts, relative to the client, from the enterprise network.
- **network-extension-mode**—Addresses of the inside hosts are accessible from the enterprise network.

Example:

```
asa(config)#vpnclient mode network-extension-mode
```

Step 4 (Optional) If desired, configure the Easy VPN hardware client to use TCP-encapsulated IPsec.

vpnclient ipsec-over-tcp [**port** *tcp_port*]

The Easy VPN hardware client uses port 10000 if not specified.

If you configure an Easy VPN Remote to use TCP-encapsulated IPsec, enter the **crypto ipsec df-bit clear-df outside** command to clear 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.

Example:

Configure the Easy VPN hardware client to use TCP-encapsulated IPsec, using the port 10501, and let it send large packets over the outside interface:

```
hostname(config)# vpnclient ipsec-over-tcp port 10501
hostname(config)# crypto ipsec df-bit clear-df outside
```

Step 5 Identify the tunnel group, configured on the Easy VPN Server, using one of the following methods:

- Specify the Easy VPN Server group policy name and password (pre-shared key).

  vpnclient vpngroup *group_name* **password** *preshared_key*

  - *group_name*—name of the VPN tunnel group configured on the Easy VPN server. You must configure this tunnel group on the server before establishing a connection.
  - *preshared_key*—the IKE pre-shared key used for authentication on the Easy VPN Server.

  For example, enter the following command to identify the VPN tunnel group named TestGroup1 and the IKE pre-shared key my_key123.

  ```
  hostname(config)# vpnclient vpngroup TestGroup1 password my_key123
  hostname(config)#
  ```

- Specify a per-configured trust point to select and authenticate the group policy.

  vpnclient trustpoint *trustpoint_name* [**chain**]

  - *trustpoint_name*—names the trustpoint identifying the RSA certificate to use for authentication.

- **chain**(Optional)—sends the entire certificate chain.

For example, enter the following command to specify the identity certificate named central and send the entire certificate chain:

```
hostname(config)# crypto ca trustpoint central
hostname(config)# vpnclient trustpoint central chain
hostname(config)#
```

Step 6 If NEM and split-tunneling are configured in the group policy, configure the VPN tunnel to autoconnect.

vpnclient nem-st-autoconnect

Step 7 (Optional) If Individual User Authentication (IAU) and IP Phone Bypass is configured in the group policy on the Easy VPN Server, exempt devices such as Cisco IP phones, wireless access points, and printers, from authentication since they are incapable of authenticating.

vpnclient mac-exempt *mac_addr_1 mac_mask_1* [*mac_addr_2 mac_mask_2...mac_addr_n mac_mask_n*]

- The list of addresses cannot exceed 15.
- *mac_addr*—the MAC address, in dotted hexadecimal notation, of the device to bypass individual user authentication.
- *mac_mask*—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.

  Only the first six characters of the specific MAC address are required if you use the MAC mask ffff.ff00.0000 to specify all devices by the same manufacturer.

Example:

Cisco IP phones have the Manufacturer ID 00036b, so the following command exempts any Cisco IP phone, including Cisco IP phones, you might add in the future:

```
hostname(config)# vpnclient mac-exempt 0003.6b00.0000 ffff.ff00.0000
hostname(config)#
```

Note
Individual User Authentication and IP Phone Bypass must be configured on the Easy VPN Server group policy as shown:

```
hostname(config-group-policy)#user-authentication enable
hostname(config-group-policy)#ip-phone-bypass enable
```

Step 8 Configure automatic Xauth user login credentials.

vpnclient username *username* **password** *password*

Step 9 (Optional) Configure Remote Management of the Easy VPN Remote.

By default, management tunnels use IPsec encryption within SSH or HTTPS encryption. Use one of the following commands to remove the IPsec encryption or retain this encryption and only allow certain hosts to manage the ASA.

- **vpnclient management clear**

Clears the IPsec encryption layer allowing management access outside of the VPN tunnel.

- **vpnclient management tunnel ip_addr_1 ip_mask_1** [*ip_addr_2 ip_mask_2...ip_addr_n ip_mask_n*]

Example:

Enter the following command to automate the creation of an IPsec tunnel to provide management access to the host with IP address 192.168.10.10:

```
hostname(config)# vpnclient management tunnel 192.198.10.10 255.255.255.0
```

Note
Do not configure a management tunnel on a ASA Easy VPN Remote if a NAT device is operating between it and the Internet. In that configuration, clear remote management using the **vpnclient management clear** command.

Step 10 Enable the Easy VPN hardware client on the ASA.

vpnclient enable

The server address(es), mode, and tunnel group specification must be configured before you can enable Easy VPN Remote.

Step 11 (Optional) Manually connect the Easy VPN tunnel if your configuration requires this.

vpnclient connect

Configure Easy VPN Server

Before you begin

Ensure all secondary Easy VPN Servers are configured with the identical options and settings as the primary Easy VPN Server.

Procedure

Step 1 Configure the Easy VPN Server for IPsec IKEv1 support. See Connection Profiles, Group Policies, and Users.

Step 2 Set the specific Easy VPN Server atttributes. See Configure Attributes for VPN Hardware Clients.

Feature History for Easy VPN

Feature Name	Releases	Feature Information
Cisco Easy VPN client on the ASA 5506-X, 5506W-X, 5506H-X, and 5508-X	9.5(1)	This release supports Cisco Easy VPN on the ASA 5 series and for the ASA 5508-X. The ASA acts as a V hardware client when connecting to the VPN header devices (computers, printers, and so on) behind the A Easy VPN port can communicate over the VPN; the have to run VPN clients individually. Note that only interface can act as the Easy VPN port; to connect m devices to that port, you need to place a Layer 2 swi port, and then connect your devices to the switch. We introduced the following commands: **vpnclient vpnclient server, vpnclient mode, vpnclient usern vpnclient ipsec-over-tcp, vpnclient management, vpngroup, vpnclient trustpoint, vpnclient nem-st-autoconnect, vpnclient mac-exempt**
Easy VPN Enhancements for BVI Support	9.9(2)	Easy VPN has been enhanced to support a Bridged V Interface as its internal secure interface, and adminis now allowed to directly configure the internal secure using the new **vpnclient secure interface** [*interface* command. A physical interface, or a Bridged Virtual Interface c assigned as the internal secure interface. If this is not administrator, Easy VPN will choose its internal secur using security levels as before, whether it is an indep physical interface or a BVI. Also, management services, such as **telnet**, **http**, an now be configured on a BVI if management access l enabled on that BVI. New or Modified commands: **vpnclient secure inte** [*interface-name*], **https**, **telnet**, **ssh**, **management-a**