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

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. In ASDM, go to **Configuration > VPN > Easy VPN Remote** to configure the ASA as an Easy VPN Remote hardware client. Go to **Configuration > Remote Access > Network (Client) Access > Group Policies > Advanced > IPsec(IKEv1) Client > Hardware Client** to configure group policy attributes on the Easy VPN Server.

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. 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. 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.

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. 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.

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.

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 Server.
- 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 Server.

  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 on the Easy VPN Server and MAC address exemption 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.

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. 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.

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.

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

Configure an ASA as an Easy VPN Remote hardware client.

Note Only the Cisco ASA with FirePOWER- 5506-X, 5506W-X, 5506H-X, and 5508-X models can be configured as an Easy VPN Remote hardware client.

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.

Configuration > VPN > Easy VPN Remote

Enable Easy VPN Remote—Enables the Easy VPN Remote feature and makes available the rest of the fields in this dialog box for configuration.

Mode—Selects either Client mode or 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**—Makes those addresses accessible from the enterprise network.

Note If the Easy VPN Remote is using NEM and has connections to secondary servers, establish an ASDM connection to each headend and check Enable Reverse Route Injection on the crypto map you created on Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Crypto Maps to configure dynamic announcements of the remote network using RRI.

- **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.

Group Settings—Specifies whether to use a pre-shared key or an X.509 certificate for user authentication.

- **Pre-shared key**—Enables the use of a 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.
  - **Group Name**—Specifies the name of the group policy to use for authentication.
  - **Group Password**—Specifies the password to use with the specified group policy.
  - **Confirm Password**—Requires you to confirm the group password just entered.
- **X.509 Certificate**—Specifies the use of an X.509 digital certificate, supplied by a Certificate Authority, for authentication.
  - **Select Trustpoint**—Lets you select a trustpoint, which can be an IP address or a hostname, from the drop-down list. To define a trustpoint, click the link to Trustpoint(s) configuration at the bottom of this area.
  - **Send certificate chain**—Enables sending a certificate chain, not just the certificate itself. This action includes the root certificate and any subordinate CA certificates in the transmission.

User Settings—Configures user login information.

- **User Name**—Configures the VPN username for the Easy VPN Remote connection. 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 Xauth username and password parameters are used when secure unit authentication is disabled and the server requests Xauth credentials. If secure unit authentication is enabled, these parameters are ignored, and the ASA prompts the user for a username and password.
- **User Password** and **Confirm Password**—Configures and confirms the VPN user password for the Easy VPN Remote connection.

Easy VPN Server To Be Added—Adds or removes an Easy VPN server. Any ASA can act as a Easy VPN server. A server must be configured before a connection can be established. The ASA supports IPv4 addresses, the names database, or DNS names and resolves addresses in that order. The first server in the Easy VPN Server(s) list is the primary server. You can specify a maximum of ten backup servers in addition to the primary server.

- **Easy VPN Server(s)**—Lists the configured Easy VPN servers in priority order.
- **Name or IP Address**—The name or IP address of an Easy VPN server to add to the list.
- **Add** and **Remove**—Moves and removes the specified server to the Easy VPN Server(s) list.
- **Move Up** and **Move Down**—Changes the position of a server in the Easy VPN Server(s) list. These buttons are available only when there is more than one server in the list.

Secure Client Interface—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, select one from the drop-down choices. A physical or virtual interface can be assigned.

Configuration > VPN > Easy VPN Remote > Advanced

MAC Exemption—Configures a set of MAC addresses and masks used for device pass-through for the Easy VPN Remote connection. Certain devices like Cisco IP phones, printers, and the like are incapable of performing authentication, and therefore of participating in individual unit authentication. To accommodate these devices, the device pass-through feature, enabled by the MAC Exemption attributes, exempts devices with the specified MAC addresses from authentication when Individual User Authentication is enabled.

- **MAC Address**—Exempts the device with the specified MAC address from authentication.

  The format for specifying the MAC address this field uses three hex digits, separated by periods; for example, 45ab.ff36.9999. The first 24 bits of the MAC address indicate the manufacturer of the piece of equipment. The last 24 bits are the unit's serial number in hexadecimal format.

- **MAC Mask**—The format for specifying the MAC mask in this field uses three hex digits, separated by periods; for example, the MAC mask ffff.ffff.ffff matches just the specified MAC address. A MAC mask of all zeroes matches no MAC address, and a MAC mask of ffff.ff00.0000 matches all devices made by the same manufacturer.

- **Add** and **Remove**—Adds or removes the specified MAC address and mask pair to the MAC Address/Mask list.

Tunneled Management—Configures IPsec encryption for device management and specifies the network or networks allowed to manage the Easy VPN hardware client connection through the tunnel.

- **Enable Tunneled Management**—Adds a layer of IPsec encryption to the SSH or HTTPS encryption already present in the management tunnel.

- **Clear Tunneled Management**—Uses the encryption already present in the management tunnel, without additional encryption. Selecting Clear Tunneled Management merely removes that IPsec encryption level and does not affect any other encryption, such as SSH or HTTP, that exists on the connection.

- **IP Address/Mask**—Lists the configured IP address and mask pairs to be operated on by the Enable or Clear functions in this area.

  - **IP Address**—Specifies the IP address of the host or network to which you want to grant administrative access to the Easy VPN hardware client through the VPN tunnel.

  - **Mask**—Specifies the network mask for the corresponding IP address.

  - **Add/Remove**—Moves or removes the specified IP address and mask to the IP Address/Mask list.

IPsec Over TCP—Configure the Easy VPN Remote connection to use PCT-encapsulated IPsec.

Note You must configure the ASA to send large packets if you configure the Easy VPN Remote connection to use PCT-encapsulated IPsec.

Go to **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > IPsec Fragmentation Policies**, double-click the outside interface, and set the DF Bit Setting Policy to Clear.

- **Enable**—Enables IPsec over TCP.
- **Enter Port Number**—Specifies the port number to use for the IPsec over TCP connection.

Server Certificate—Configures the Easy VPN Remote connection to accept only connections to Easy VPN servers with the specific certificates specified by the certificate map. Use this parameter to enable Easy VPN server certificate filtering.

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 General VPN Setup.

Step 2 Set the specific Easy VPN Server atttributes. See Internal Group Policy, Hardware Client Attributes for IPsec (IKEv1).

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 AS series and for the ASA 5508-X. The ASA acts as hardware client when connecting to the VPN hea devices (computers, printers, and so on) behind th Easy VPN port can communicate over the VPN; have to run VPN clients individually. Note that c interface can act as the Easy VPN port; to conne devices to that port, you need to place a Layer 2 port, and then connect your devices to the switch We introduced the following screen: **Configurat Easy VPN Remote**

Feature Name	Releases	Feature Information
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.