



## CHAPTER 2

# Configuring the VPN Client Using ASDM

---

This chapter describes how to use the Adaptive Security Device Manager “ASDM) to configure the VPN Client on an Adaptive Security Appliance. It comprises the following sections:

- [Configuring IPsec Remote Access Connection Profiles, page 2-1](#)
- [IKE Parameters, page 2-9](#)
- [Configuring Client Software Update Using ASDM, page 2-13](#)
- [Configuring Group Policies for IPsec Client Connections Using ASDM, page 2-16](#)
- [Configuring Advanced IPsec Client Parameters, page 2-20](#)

## Configuring IPsec Remote Access Connection Profiles

To configure the security appliance for use with the VPN Client, you must configure the appropriate parameters under Configuration > Remote Access VPN > Network (Client) Access > IPsec Connection Profiles, Group Policies, and Advanced.

This section describes the elements of the security appliance configuration process specifically relevant to the VPN Client. You must also configure (or accept the default values for) the rest of the parameters, as described in the ASDM online help, the ASDM User Manual, and the ASA CLI Configuration Guide.

The IPsec group uses the IPsec connection parameters to create a tunnel. An IPsec connection can be either remote-access or site-to-site. This chapter deals only with remote-access connections, though, for the sake of completeness, site-to-site connections are mentioned where appropriate. The IPsec group is configured on the internal server or on an external RADIUS server. For ASA 5505 in client mode or VPN 3002 hardware client parameters, which enable or disable interactive hardware client authentication and individual user authentication, the IPsec connection parameters take precedence over parameters set for users and groups.

If there are no connection profiles configured, or if you want to change an existing connection profile, click Add or Edit, as appropriate.



### Note

---

The terms “connection profile” and “tunnel group” are sometimes used interchangeably.

---

To configure IPsec connection profiles, select Configuration > Remote Access VPN > Network (Client) Access > IPsec Connection Profiles. The parameters in the IPsec Connection Profiles window let you configure IPsec remote access connections. Most of the parameters in this section were formerly configured under tunnel groups. An IPsec connection represents a connection-specific record for IPsec and Clientless SSL VPN connections. Perform the following steps:

- 
- Step 1** In the Access Interfaces area, select the interfaces to enable for IPsec access. The default is that no access is selected.
- Step 2** The Connection Profiles area shows in tabular format the configured parameters for existing IPsec connections. The Connection Profiles table contains records that determine connection policies. A record identifies a default group policy for the connection and contains protocol-specific connection parameters. The table contains the following columns:
- Name—Specifies the name or IP address of the IPsec connection.
  - ID Certificate—Specifies the name of the ID certificate, if available.
  - IPsec Protocol—Indicates whether the IPsec protocol is enabled. You enable this protocol on the Add or Edit IPsec Remote Access Connection, Basic window.
  - L2TP/IPsec Protocol—Indicates whether the L2TP/IPsec protocol is enabled. You enable this protocol on the Add or Edit IPsec Remote Access Connection, Basic window.
  - Group Policy—Indicates the name of the group policy for this IPsec connection.
- Step 3** Select the IPsec Enabled check box to enable IPsec for each appropriate connection.
- 

If you want to add a new connection profile or modify an existing, selected one, click Add or Edit. These open the Add or Edit IPsec Remote Access Connection Profile dialog box.

To remove the selected server group from the table, click Delete. There is no confirmation or undo.

## Adding or Editing an IPsec Connection Profile

The Add or Edit IPsec Remote Access Connection Profile Basic dialog box lets you configure common attributes for IPsec connections. The navigation pane at the left of the dialog box lets you select whether you want to configure Basic or Advanced connection profile attributes.

## Configuring Basic Attributes

Begin with the Basic attributes. The fields to configure are as follows:

### Fields

- Name—Identifies the name of the connection. For the Edit function, this field is read-only.
- IKE Peer Authentication—Configures IKE peers.
  - Pre-shared key—Specifies the value of the pre-shared key for the connection. The maximum length of a pre-shared key is 128 characters.
  - Identity Certificate—Selects the name of an identity certificate, if any identity certificates are configured and enrolled.
  - Manage—Opens the Manage Identity Certificates window, on which you can add, edit, delete, export, and show details for a selected certificate.
- User Authentication—Specifies information about the servers used for user authentication. You can configure more authentication information in the Advanced section.

- Server Group—Selects the server group to use for user authentication. the default is LOCAL. If you select something other than LOCAL, the Fallback check box becomes available.
- Manage—Opens the Configure AAA Server Groups dialog box.
- Fallback—Specifies whether to use LOCAL for user authentication if the specified server group fails.
- Client Address Assignment—Specifies attributes relevant to assigning client attributes.
  - DHCP Servers—Specifies the IP address of a DHCP server to use. You can add up to 10 servers, separated by spaces.
  - Client Address Pools—Specifies up to 6 predefined address pools. To define an address pool, go to Configuration > Remote Access VPN > Network Client Access > Address Assignment > Address Pools.
  - Select—Opens the Select Address Pools dialog box, on which you can select, add, or edit an address pool. Double-click your selection so that it appears in the Assigned Address Pools field. You can assign more than one address pool for a connection. When assigned, your selection appears in the Client Address Pools field.
- Default Group Policy—Specifies attributes relevant to the default group policy.
  - Group Policy—Selects the default group policy to use for this connection. The default is DfltGrpPolicy.
  - Manage—Opens the Configure Group Policies dialog box, from which you can add, edit, or delete group policies.
  - Client Protocols—Selects the protocol or protocols to use for this connection. By default, both IPsec and L2TP over IPsec are selected. Ensure that Enable IPsec protocol is selected.

## Configuring Advanced Attributes

The Advanced attributes configure general, client addressing, authentication, authorization, accounting, IPsec, and PPP information for the connection profile. While you must configure (or accept the default values) for all the attributes, this section describes only those attributes that directly affect IPsec connections.

## Configuring Client Addressing

To specify the client IP address assignment policy and assign address pools to all IPsec and SSL VPN connections, choose Configuration > Remote Access VPN > Network (Client) Access > IPsec or SSL VPN Connections > Add or Edit > Advanced > Client Addressing. The Add IPsec Remote Access Connection dialog box opens. Use this dialog box to add address pools and assign them to interfaces, and view, edit, or delete them. The table lists the configured interface-specific address pools.



**Note** You cannot modify or remove an address pool if it is already in use. If you click Edit and the address pool is in use, ASDM displays an error message and lists the connection names and usernames that are using the addresses in the pool.

Use the following sections to understand and assign values to the fields in the Add IPsec Remote Access Connection window and its descendent windows:

- [Add or Edit IPsec Remote Access Connection and Add SSL VPN Access Connection, page 2-4](#)

- [Assigning Address Pools to an Interface, page 2-4](#)
- [Select Address Pools, page 2-5](#)
- [Add or Edit IP Pool, page 2-5](#)

## Add or Edit IPsec Remote Access Connection and Add SSL VPN Access Connection

To access the Add or Edit IPsec Remote Access Connection Profile window, choose Configuration > Remote Access VPN > Network (Client) Access > IPsec or SSL VPN Connections > Add or Edit > Advanced > Client Addressing.

### Fields

Use the following descriptions to assign values to the fields in this window:

- Global Client Address Assignment Policy—Configures a policy that affects all IPsec and SSL VPN Client connections (including AnyConnect client connections). The security appliance uses the selected sources in order, until it finds an address:
  - Use authentication server—Specifies that the security appliance should attempt to use the authentication server as the source for a client address.
  - Use DHCP—Specifies that the security appliance should attempt to use DHCP as the source for a client address.
  - Use address pool—Specifies that the security appliance should attempt to use address pools as the source for a client address.
- Interface-Specific Address Pools—Lists the configured interface-specific address pools.
- Add or Edit—Opens the Assign Address Pools to Interface dialog box, on which you can view, add, or modify the address pool assignments, as described in the following section.
- Delete—Removes an address-pool assignment from the table.

## Assigning Address Pools to an Interface

Use the Assign Address Pools to Interface window to select an interface and assign one or more address pools to that interface. To access this window, choose Configure > Remote Access VPN > Network (Client) Access > IPsec or SSL VPN Connections > Add or Edit > Advanced > Client Addressing > Add or Edit.

### Fields

Use the following descriptions to assign values to the fields in this window:

- Interface—Select the interface to which you want to assign an address pool. The default is DMZ.
- Address Pools—Specify an address pool to assign to the specified interface.
- Select—Opens the Select Address Pools dialog box, on which you can select one or more address pools to assign to this interface. Your selection appears in the Address Pools field of the Assign Address Pools to Interface dialog box.

## Select Address Pools

The Select Address Pools window shows the pool name, starting and ending addresses, and subnet mask of address pools available for client address assignment and lets you add, edit, or delete entries from that list. To access this window, choose Configuration > Remote Access VPN > Network (Client) Access > IPsec or SSL VPN Connections > Add or Edit > Advanced > Client Addressing > Add or Edit > Select.

### Fields

Use the following descriptions to assign values to the fields in this window:

- Add—Opens the Add IP Pool window, on which you can configure a new IP address pool.
- Edit—Opens the Edit IP Pool window, on which you can modify a selected IP address pool.
- Delete—Removes the selected address pool. There is no confirmation or undo.
- Assign—Displays the address pool names that remained assigned to the interface. Select a pool from the table and click Assign or double-click each unassigned pool you want to add to the interface. The Assign field updates the list of pool assignments on the Assign Address Pools to Interface dialog box.

## Add or Edit IP Pool

The Add or Edit IP Pool dialog box lets you specify or modify a range of IP addresses for client address assignment. To access this dialog box, choose Configuration > Remote Access VPN > Network (Client) Access > IPsec or SSL VPN Connections > Add or Edit > Advanced > Client Addressing > Add or Edit > Select > Add or Edit.

### Fields

Use the following descriptions to assign values to the fields in this window:

- Name—Specifies the name assigned to the IP address pool.
- Starting IP Address—Specifies the first IP address in the pool.
- Ending IP Address—Specifies the last IP address in the pool.
- Subnet Mask—Selects the subnet mask to apply to the addresses in the pool.

## Configuring IPsec-specific Parameters

To configure IPsec-specific parameters, start by selecting Configuration > Remote Access VPN > Network (Client) Access > IPsec Connection Profiles, then do the following steps:

- 
- Step 1** In the Access Interfaces area, check the appropriate boxes to enable specific interfaces for IPsec access. Only interfaces that have already been configured appear in this selection box.
  - Step 2** In the Connection Profiles area, check the check box under IPsec Enabled for each connection profile (tunnel group) that uses IPsec.
  - Step 3** To Add a connection profile to this list, click Add. You can then go back and configure all of the connection profile parameters. See [Configuring IPsec Remote Access Connection Profiles, page 2-1](#) for details.

- Step 4** To modify an existing connection profile, click Edit. See [Modifying an Existing IPsec Connection Profile, page 2-6](#).
- Step 5** To remove a connection profile from this list, click Delete.
- Step 6** Click Apply. The changes are saved to the running configuration.
- 

## Modifying an Existing IPsec Connection Profile

The Add or Edit IPsec Connection Profile window lets you configure or edit IPsec-specific connection-profile parameters, as previously described.

### Fields

- Send certificate chain—Enables or disables sending the entire certificate chain. This action includes the root certificate and any subordinate CA certificates in the transmission.
- IKE Peer ID Validation—Selects whether IKE peer ID validation is ignored, required, or checked only if supported by a certificate.
- IKE Keep Alive—Enables and configures ISAKMP keep alive monitoring.
  - Disable Keep Alives—Enables or disables ISAKMP keep alives.
  - Monitor Keep Alives—Enables or disables ISAKMP keep alive monitoring. Selecting this option makes available the Confidence Interval and Retry Interval fields.
  - Confidence Interval—Specifies the ISAKMP keep alive confidence interval. This is the number of seconds the security appliance should allow a peer to idle before beginning keepalive monitoring. The minimum is 10 seconds; the maximum is 300 seconds. The default for a remote access group is 300 seconds.
  - Retry Interval—Specifies number of seconds to wait between ISAKMP keep alive retries. The default is 2 seconds.
  - Head end will never initiate keepalive monitoring—Specifies that the central-site security appliance never initiates keepalive monitoring.
- Interface-Specific Authentication Mode—Specifies the authentication mode on a per-interface basis.
  - Interface—Lets you select the interface name. The default interfaces are inside and outside, but if you have configured a different interface name, that name also appears in the list.
  - Authentication Mode—Lets you select the authentication mode, none, xauth, or hybrid, as above.
  - Interface/Authentication Mode table—Shows the interface names and their associated authentication modes that are selected.
  - Add or Edit—Adds or modifies an interface/authentication mode pair selection in the Interface/Authentication Modes table.
  - Delete—Removes an interface/authentication mode pair selection from the Interface/Authentication Modes table.
- Client VPN Software Update Table—Lists the client type, VPN Client revisions, and image URL for each client VPN software package installed. For each client type, you can specify the acceptable client software revisions and the URL or IP address from which to download software upgrades, if necessary. The client update mechanism (described in detail under the Client Update window) uses

this information to determine whether the software each VPN client is running is at an appropriate revision level and, if appropriate, to provide a notification message and an update mechanism to clients that are running outdated software.

- Client Type—Identifies the VPN client type. “Windows” includes all Windows-based platforms. “Win NT” includes Windows Vista, Windows XP, Windows 2000, and Windows NT 4.0. The other platforms are Linux, Solaris, and Mac OS X. The VPN Client, release 5.0 and higher, does not support the Windows 95, Windows 98, and Windows ME platforms.



**Note** The secure gateway sends a separate notification message for each entry in a Client Update list; therefore, your client update entries must not overlap. For example, the value “Windows” includes all Windows platforms, and the value “WinNT” includes Windows Vista, Windows XP, Windows 2000, and Windows NT 4.0, so you cannot specify both Windows and Windows NT. To find out the client types and version information, click the lock icon in the top left corner of the Cisco Systems VPN Client main window and choose “About VPN Client.”

- VPN Client Revisions—Specifies the acceptable revision level of the VPN client.
- Image URL—Specifies the URL or IP address from which the correct VPN client software image can be downloaded. For Windows-based VPN clients, the URL must be of the form `http://` or `https://`. For ASA 5505 in client mode or VPN 3002 hardware clients, the URL must be of the form `tftp://`.

## Configuring IKE Authentication Mode

Configure the default and interface-specific IKE authentication modes on the Configuration > Remote Access VPN > Network (Client) Access > IPsec Connection Profiles > Advanced > IPsec > IKE Authentication window by performing the following steps:

**Step 1** Set the default mode: XAUTH, Hybrid XAUTH, or Disable user authentication during IKE.

- XAUTH—Specifies the use of IKE Extended Authentication mode, which provides the capability of authenticating a user within IKE using TACACS+ or RADIUS. This is the default value.
- Hybrid XAUTH—Specifies the use of Hybrid mode, which lets you use digital certificates for security appliance authentication and a different, legacy method—such as RADIUS, TACACS+ or SecurID—for remote VPN user authentication. This mode breaks phase 1 of the Internet Key Exchange (IKE) into the following steps, together called hybrid authentication:

The security appliance authenticates to the remote VPN user with standard public key techniques. This establishes an IKE security association that is unidirectionally authenticated.

An extended authentication (xauth) exchange then authenticates the remote VPN user. This extended authentication can use one of the supported legacy authentication methods.



**Note** Before setting the authentication type to hybrid, you must configure the authentication server and create a pre-shared key.

- Disable user authentication during IKE—If you enable reauthentication on IKE rekey, the security appliance prompts the user to enter a username and password during initial Phase 1 IKE negotiation and also prompts for user authentication whenever an IKE rekey occurs. Reauthentication provides

additional security. If the configured rekey interval is very short, users might find the repeated authorization requests inconvenient. To avoid repeated authorization requests, disable reauthentication during IKE.

- Step 2** Specify whether to include the “Enter Username and Password” prompt in the XAUTH request.
- Step 3** To Add a connection profile to this list, click Add. To modify an existing connection profile, click Edit. To remove a connection profile from this list, click Delete.
- Step 4** Click Apply. The changes are saved to the running configuration.

## Adding or Editing a Connection Profile IKE Authentication Entry

Internet Key Exchange (IKE) establishes a shared security policy and authenticates keys for services (such as IPsec) that require keys. Before any IPsec traffic can be passed, each security appliance must verify the identity of its peer. This can be done by manually entering preshared keys into both hosts or by a CA service. IKE is a hybrid protocol that uses part Oakley and part of another protocol suite called SKEME inside the ISAKMP framework. This is the protocol formerly known as ISAKMP/Oakley, and is defined in RFC 2409.

You must enable IKE for each interface that you want to use for VPN connections.



### Note

VPN Client connections are not supported if you configure the **crypto isakmp keepalive** command with the periodic keyword (for example, **crypto isakmp keepalive timeoutval periodic**) on an IOS device.

IKE Extended Authenticate (XAUTH) is implemented per the IETF draft-ietf-ipsec-isakmp-xauth-04.txt (“extended authentication” draft). This protocol provides the capability of authenticating a user within IKE using TACACS+ or RADIUS.

Set the default mode for user authentication on the drop-down menu. The options are XAUTH (Extended user authentication), Hybrid XAUTH, and Disable user authentication during IKE. The default value is XAUTH.

XAUTH authenticates a user within IKE using TACACS+ or RADIUS. XAUTH authenticates a user using RADIUS or any of the other supported user authentication protocols.

Use hybrid XAUTH authentication when you need to use digital certificates for security appliance authentication and a different, legacy method for remote VPN user authentication, such as RADIUS, TACACS+ or SecurID.

Hybrid XAUTH breaks phase 1 of IKE down into the following two steps, together called hybrid authentication:

- The security appliance authenticates to the remote VPN user with standard public key techniques. This establishes an IKE security association that is unidirectionally authenticated.
- An XAUTH exchange then authenticates the remote VPN user. This extended authentication can use one of the supported legacy authentication methods.



### Note

Before setting the authentication type hybrid, you must configure the authentication server, create a preshared key, and configure a trustpoint.

To Add or Edit a specific interface on which to apply IKE authentication, do the following steps:

- 
- Step 1** In the Interface-Specific Mode area, click Add or Edit. The Assign Authentication Mode to Interface dialog box appears.
- Step 2** Select the interface from the drop-down menu.
- Step 3** Select the authentication mode to use. The choices are XAUTH, Hybrid XAUTH, and Disable user authentication during IKE, as explained above.
- Step 4** Click OK. Your choices appear in the Interface-Specific Mode area.
- Step 5** Click OK to apply your selections.
- 

## IKE Parameters

To enable IKE parameters, select Configuration > Remote Access VPN. This panel lets you set system wide values for VPN connections. The following sections describe each of the options.

### Enabling IKE on Interfaces

You must enable IKE for each interface that you want to use for VPN connections.

### Enabling IPsec over NAT-T

NAT-T lets IPsec peers establish both remote access and site-to-site connections through a NAT device. It does this by encapsulating IPsec traffic in UDP datagrams, using port 4500, thereby providing NAT devices with port information. NAT-T auto-detects any NAT devices, and only encapsulates IPsec traffic when necessary. This feature is disabled by default.

- The security appliance can simultaneously support standard IPsec, IPsec over TCP, NAT-T, and IPsec over UDP, depending on the client with which it is exchanging data.
- When both NAT-T and IPsec over UDP are enabled, NAT-T takes precedence.
- When enabled, IPsec over TCP takes precedence over all other connection methods.

The security appliance implementation of NAT-T supports IPsec peers behind a single NAT/PAT device as follows:

- One site-to-site connection.
- Either a site-to-site connection or multiple remote access clients, but not a mixture of both.

To use NAT-T you must:

- Open port 4500 on the security appliance.
- Enable IPsec over NAT-T globally in this panel.
- Select the second or third option for the Fragmentation Policy parameter in the Configuration > VPN > IPsec > Pre-Fragmentation panel. These options let traffic travel across NAT devices that do not support IP fragmentation; they do not impede the operation of NAT devices that do support IP fragmentation.

## Enabling IPsec over TCP

IPsec over TCP enables a VPN client to operate in an environment in which standard ESP or IKE cannot function, or can function only with modification to existing firewall rules. IPsec over TCP encapsulates both the IKE and IPsec protocols within a TCP packet, and enables secure tunneling through both NAT and PAT devices and firewalls. This feature is disabled by default.



### Note

This feature does not work with proxy-based firewalls.

IPsec over TCP works with remote access clients. It works on all physical and VLAN interfaces. It is a client to security appliance feature only. It does not work for site-to-site connections.

- The security appliance can simultaneously support standard IPsec, IPsec over TCP, NAT-Traversal, and IPsec over UDP, depending on the client with which it is exchanging data.
- The VPN 3002 hardware client, which supports one tunnel at a time, can connect using standard IPsec, IPsec over TCP, NAT-Traversal, or IPsec over UDP.
- When enabled, IPsec over TCP takes precedence over all other connection methods.

You enable IPsec over TCP on both the security appliance and the client to which it connects.

You can enable IPsec over TCP for up to 10 ports that you specify. If you enter a well-known port, for example port 80 (HTTP) or port 443 (HTTPS), the system displays a warning that the protocol associated with that port will no longer work. The consequence is that you can no longer use a browser to manage the security appliance through the IKE-enabled interface. To solve this problem, reconfigure the HTTP/HTTPS management to different ports.

You must configure TCP port(s) on the client as well as on the security appliance. The client configuration must include at least one of the ports you set for the security appliance.

## Determining ID Method

During IKE negotiations the peers must identify themselves to each other. You can choose the identification methods from the following options:

**Table 2-1** *IKE Identification Methods*

Parameter	Use
Address	Uses the IP addresses of the hosts exchanging ISAKMP identity information.
Hostname	Uses the fully-qualified domain name of the hosts exchanging ISAKMP identity information (default). This name comprises the hostname and the domain name.
Key ID	Uses the string the remote peer uses to look up the preshared key.
Automatic	Determines IKE negotiation by connection type: <ul style="list-style-type: none"> <li>• IP address for preshared key</li> <li>• Cert DN for certificate authentication.</li> </ul>

## Disabling Inbound Aggressive Mode Connections

Phase 1 IKE negotiations can use either Main mode or Aggressive mode. Both provide the same services, but Aggressive mode requires only two exchanges between the peers, rather than three. Aggressive mode is faster, but does not provide identity protection for the communicating parties. It is therefore necessary that they exchange identification information prior to establishing a secure SA in which to encrypt information. This feature is disabled by default.

## Alerting Peers Before Disconnecting

Client or site-to-site sessions might be dropped for several reasons, such as: a security appliance shutdown or reboot, session idle timeout, maximum connection time exceeded, or administrator cut-off.

The security appliance can notify qualified peers (in site-to-site configurations), VPN Clients and VPN 3002 Hardware Clients of sessions that are about to be disconnected, and it conveys to them the reason. The peer or client receiving the alert decodes the reason and displays it in the event log or in a pop-up panel. This feature is disabled by default.

This panel lets you enable the feature so that the security appliance sends these alerts, and conveys the reason for the disconnect.

Qualified clients and peers include the following:

- Security appliance devices with Alerts enabled.
- VPN clients running 4.0 or later software (no configuration required).
- VPN 3002 hardware clients running 4.0 or later software, and with Alerts enabled.
- VPN 3000 Series Concentrators running 4.0 or later software, with Alerts enabled.

This feature does not apply to the following clients:

- Cisco AnyConnect VPN Client
- Cisco IOS software
- Cisco Secure PIX Firewall

## Waiting for Active Sessions to Terminate Prior to Reboot

You can schedule a central-site device reboot to occur only when all active sessions have terminated voluntarily. This feature is disabled by default.

### Fields

- Enable IKE—Shows IKE status for all configured interfaces.
  - Interface—Displays names of all configured security appliance interfaces.
  - IKE Enabled—Shows whether IKE is enabled for each configured interface.
  - Enable/Disables—Click to enable or disable IKE for the highlighted interface.
- NAT Transparency—Lets you enable or disable IPsec over NAT-T and IPsec over TCP.
  - Enable IPsec over NAT-T—Select to enable IPsec over NAT-T.

- NAT Keepalive—Type the number of seconds that can elapse with no traffic before the security appliance terminates the NAT-T session. The default is 20 seconds. The range is 10 to 3600 seconds (one hour).
- Enable IPsec over TCP—Select to enable IPsec over TCP.
- Enter up to 10 comma-separated TCP port values—Type up to 10 ports on which to enable IPsec over TCP. Use a comma to separate the ports. You do not need to use spaces. The default port is 10,000. The range is 1 to 65,635.
- Identity to Be Sent to Peer—Lets you set the way that IPsec peers identify themselves to each other. During IKE negotiations the peers must identify themselves to each other. You can choose the identification methods from the following options:
  - Identity—Select one of the following methods by which IPsec peers identify themselves:

Parameter	Function
Address	Uses the IP addresses of the hosts.
Hostname	Uses the fully-qualified domain names of the hosts. This name comprises the hostname and the domain name.
Key ID	Uses the string the remote peer uses to look up the preshared key.
Automatic	Determines IKE negotiation by connection type: IP address for preshared key or cert DN for certificate authentication.

- Key Id String—Type the alphanumeric string the peers use to look up the preshared key.
- Disable inbound aggressive mode connections—Select to disable aggressive mode connections.
- Alert peers before disconnecting—Select to have the security appliance notify qualified site-to-site peers and remote access clients before disconnecting sessions.
- Wait for all active sessions to voluntarily terminate before rebooting—Select to have the security appliance postpone a scheduled reboot until all active sessions terminate.

**Note**

If you have a site-to-site configuration using IKE main mode, make sure that the two peers have the same IKE keepalive configuration. Both peers must have IKE keepalives enabled or both peers must have it disabled.

If you configure authentication using digital certificates, you can specify whether to send the entire certificate chain (which sends the peer the identity certificate and all issuing certificates) or just the issuing certificates (including the root certificate and any subordinate CA certificates).

You can notify users who are using outdated versions of Windows client software that they need to update their client, and you can provide a mechanism for them to get the updated client version. For VPN 3002 hardware client users, you can trigger an automatic update. You can configure and change the client-update, either for all connection profiles or for particular connection profiles.

If you configure authentication using digital certificates, you can specify the name of the trustpoint that identifies the certificate to send to the IKE peer.

# Configuring Client Software Update Using ASDM

The client update feature ensures acceptable Client revision levels. This feature lets administrators at a central location automatically notify VPN client users that it is time to update the VPN client software and the VPN 3002 hardware client image.

Remote users might be using outdated VPN software or hardware client versions. You can use the client-update feature to enable updating client revisions; specify the types and revision numbers of clients to which the update applies; provide a URL or IP address from which to get the update; and, in the case of Windows clients, optionally notify users that they should update their VPN client version. For Windows clients, you can provide a mechanism for users to accomplish that update. For VPN 3002 hardware client users, the update occurs automatically, with no notification. This feature applies only to the IPsec remote-access tunnel-group type.

If the client is already running a software version that is at least as high as those included on the list of revision numbers, it does not need to update its software. If the client is not running a software version on the list (or a higher version), it should update.

The Client VPN Software Update Table lists the client type, VPN Client revisions, and image URL for each client VPN software package installed. For each client type, you can specify the acceptable client software revisions and the URL or IP address from which to download software upgrades, if necessary. The client update mechanism (described in detail under the Client Update window) uses this information to determine whether the software each VPN client is running is at an appropriate revision level and, if appropriate, to provide a notification message and an update mechanism to clients that are running outdated software. Specify the following fields to configure client update.

Configure the Client Software Update Table on the Configuration > Remote Access VPN > Network (Client) Access > IPsec Connection Profiles > Advanced > IPsec > Client Software Update window by configuring the following fields:

## Fields

- **Enable Client Update**—Enables or disables client update, both globally and for specific tunnel groups. You must enable client update before you can send a client update notification to Windows, MAC OS X, and Linux VPN clients, or initiate an automatic update to hardware clients.
- **Client Type**—Lists the clients to upgrade: software or hardware, and for Windows software clients, all Windows or a subset. If you click All Windows Based, do not specify Windows versions individually. The specification for Windows NT, Windows 2000, and Windows XP also includes Windows Vista. The hardware client gets updated with a release of the ASA 5505 software or of the VPN 3002 hardware client.

If the client update feature has already been configured to support all Windows clients, you must remove that specification before specifying individual Windows client types.



### Note

The secure gateway sends a separate notification message for each entry in a Client Update list; therefore, your client update entries must not overlap. For example, the value “Windows” includes all Windows platforms, and the value “WinNT” includes Windows Vista, Windows XP, Windows 2000, and Windows NT 4.0, so you cannot specify both Windows and Windows NT. To find out the client types and version information, click the lock icon in the top left corner of the Cisco Systems VPN Client main window and choose “About VPN Client.”

- **Client Type**—Lists the clients to upgrade: software or hardware, and for Windows software clients, all Windows or a subset. If you click All Windows Based, do not specify Windows versions individually. The specification for Windows NT, Windows 2000, and Windows XP also includes Windows Vista. The hardware client gets updated with a release of the ASA 5505 software or of the VPN 3002 hardware client.
- **VPN Client Revisions**—Contains a comma-separated list of software image revisions appropriate for this client. If the user's client revision number matches one of the specified revision numbers, there is no need to update the client, and, for Windows-based clients, the user does not receive an update notification. The following caveats apply:
  - The revision list must include the software version for this update.
  - Your entries must match exactly those on the URL for the VPN client, or the TFTP server for the hardware client.
  - The TFTP server for distributing the hardware client image must be a robust TFTP server.
  - A VPN client user must download an appropriate software version from the listed URL.
  - The VPN 3002 hardware client software is automatically updated via TFTP, with no notification to the user.
- **Image URL**—Contains the URL or IP address from which to download the software image. This URL must point to a file appropriate for this client. For Windows, MAC OS X, and Linux-based clients, the URL must be in the form: `http://` or `https://`. For hardware clients, the URL must be in the form `tftp://`.
  - For Windows, MAC OS X, and Linux-based VPN clients: To activate the Launch button on the VPN Client Notification, the URL must include the protocol HTTP or HTTPS and the server address of the site that contains the update. The format of the URL is: `http(s)://server_address:port/directory/filename`. The server address can be either an IP address or a hostname if you have configured a DNS server. For example:
 

```
http://10.10.99.70/vpnclient-win-4.6.Rel-k9.exe
```

The directory is optional. You need the port number only if you use ports other than 80 for HTTP or 443 for HTTPS.
  - For the hardware client: The format of the URL is `tftp://server_address/directory/filename`. The server address can be either an IP address or a hostname if you have configured a DNS server. For example:
 

```
tftp://10.1.1.1/vpn3002-4.1.Rel-k9.bin
```

## Enabling Client Update

To enable IPsec VPN Client update and, optionally, upgrade connected clients, select Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Upload Software > Client Software.

The Client Software dialog box lets administrators at a central location do the following actions:

- Enable client update; specify the types and revision numbers of clients to which the update applies.
- Provide a URL or IP address from which to get the update.
- In the case of Windows clients, optionally notify users that they should update their VPN client version.

**Note**

The Client Update function at Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Upload Software > Client Software applies only to the (IPsec) Cisco VPN Client, (for Windows, MAC OS X, and Linux), and the VPN 3002 hardware client. It does not apply to the Cisco AnyConnect VPN clients, which is automatically updated by the security appliance when it connects.

For the IPsec VPN Client, you can provide a mechanism for users to accomplish that update. For VPN 3002 hardware client users, the update occurs automatically, with no notification. You can apply client updates only to the IPsec remote-access tunnel-group type.

**Note**

If you try to do a client update to an IPsec site-to-site IPsec connection or a Clientless VPN IPsec connection, you do not receive an error message, but no update notification or client update goes to those types of IPsec connections.

To enable client update globally for all clients of a particular client type, use this window. You can also notify all Windows, MAC OS X, and Linux clients that an upgrade is needed and initiate an upgrade on all VPN 3002 hardware clients from this window. To configure the client revisions to which the update applies and the URL or IP address from which to download the update, click Edit.

To configure client update revisions and software update sources for a specific tunnel group, see Configuration > Remote Access VPN > Network (Client) Access > IPsec > Add/Edit > Advanced > IPsec > Client Software Update.

**Fields**

- **Enable Client Update**—Enables or disables client update, both globally and for specific tunnel groups. You must enable client update before you can send a client update notification to Windows, MAC OS X, and Linux VPN clients, or initiate an automatic update to hardware clients.
- **Client Type**—Lists the clients to upgrade: software or hardware, and for Windows software clients, all Windows or a subset. If you click All Windows Based, do not specify Windows versions individually. The hardware client gets updated with a release of the ASA 5505 software or of the VPN 3002 hardware client.

**Note**

The secure gateway sends a separate notification message for each entry in a Client Update list; therefore, your client update entries must not overlap. For example, the value “Windows” includes all Windows platforms, and the value “WinNT” includes Windows Vista, Windows XP, Windows 2000, and Windows NT 4.0, so you cannot specify both Windows and Windows NT. To find out the client types and version information, click the lock icon in the top left corner of the Cisco Systems VPN Client main window and choose “About VPN Client.”

- **VPN Client Revisions**—Contains a comma-separated list of software image revisions appropriate for this client. If the user's client revision number matches one of the specified revision numbers, there is no need to update the client, and, for Windows-based clients, the user does not receive an update notification. The following caveats apply:
  - The revision list must include the software version for this update.
  - Your entries must match exactly those on the URL for the VPN client, or the TFTP server for the hardware client.
  - The TFTP server for distributing the hardware client image must be a robust TFTP server.
  - A VPN client user must download an appropriate software version from the listed URL.

- The VPN 3002 hardware client software is automatically updated via TFTP, with no notification to the user.
- Image URL—Contains the URL or IP address from which to download the software image. This URL must point to a file appropriate for this client. For Windows, MAC OS X, and Linux-based clients, the URL must be in the form: `http://` or `https://`. For hardware clients, the URL must be in the form `tftp://`.
  - For Windows, MAC OS X, and Linux-based VPN clients: To activate the Launch button on the VPN Client Notification, the URL must include the protocol HTTP or HTTPS and the server address of the site that contains the update. The format of the URL is: `http(s)://server_address:port/directory/filename`. The server address can be either an IP address or a hostname if you have configured a DNS server. For example:
 

```
http://10.10.99.70/vpnclient-win-4.6.Rel-k9.exe
```

The directory is optional. You need the port number only if you use ports other than 80 for HTTP or 443 for HTTPS.
  - For the hardware client: The format of the URL is `tftp://server_address/directory/filename`. The server address can be either an IP address or a hostname if you have configured a DNS server. For example:
 

```
tftp://10.1.1.1/vpn3002-4.1.Rel-k9.bin
```
- Edit—Opens the Edit Client Update Entry dialog box, which lets you configure or change client update parameters. See [Edit Client Update Entry](#).
- Live Client Update—Sends an upgrade notification message to all currently connected VPN clients or selected tunnel group(s).
  - Tunnel Group—Selects all or specific tunnel group(s) for updating.
  - Update Now—Immediately sends an upgrade notification containing a URL specifying where to retrieve the updated software to the currently connected VPN clients in the selected tunnel group or all connected tunnel groups. The message includes the location from which to download the new version of software. The administrator for that VPN client can then retrieve the new software version and update the VPN client software.

For VPN 3002 hardware clients, the upgrade proceeds automatically, with no notification.

You must check Enable Client Update in the window for the upgrade to work. Clients that are not connected receive the upgrade notification or automatically upgrade the next time they log on.

## Configuring Group Policies for IPsec Client Connections Using ASDM

The Group Policies window, Configuration > Remote Access VPN > Network (Client) Access > Group Policies) lets you manage the attributes for individual VPN group policies. A VPN group policy is a collection of user-oriented attribute/value pairs stored either internally on the device or externally on a RADIUS or LDAP server. Configuring the VPN group policy lets users inherit attributes that you have not configured at the individual group or username level. By default, VPN users have no group policy association. The group policy information is used by VPN tunnel groups and user accounts.

The “child” windows and dialog boxes let you configure the group parameters, including those for the default group. The default group parameters are those that are most likely to be common across all groups and users, and they streamline the configuration task. Groups can “inherit” parameters from this default group, and users can “inherit” parameters from their group or the default group. You can override these parameters as you configure groups and users.

You can configure either an internal or an external group policy. An internal group policy is stored locally, and an external group policy is stored externally on a RADIUS or LDAP server. Clicking Edit opens a similar dialog box on which you can create a new group policy or modify an existing one.

In these dialog boxes, you configure the following kinds of parameters:

- General attributes: Name, banner, address pools, protocols, filtering, and connection settings.
- Servers: DNS and WINS servers, DHCP scope, and default domain name.
- Advanced attributes: Split tunneling, IE browser proxy, SSL VPN Client and AnyConnect Client, and IPsec Client.

Before configuring these parameters, you should configure the following:

- Access hours.
- Rules and filters.
- IPsec Security Associations.
- Network lists for filtering and split tunneling
- User authentication servers, and specifically the internal authentication server.

## Fields

- Group Policy—Lists the currently configured group policies and Add, Edit, and Delete buttons to help you manage VPN group policies.
- Name—Lists the name of the currently configured group policies.
- Type—Lists the type of each currently configured group policy.
- Tunneling Protocol—Lists the tunneling protocol that each currently configured group policy uses.
- AAA Server Group—Lists the AAA server group, if any, to which each currently configured group policy pertains.
- Add—Offers a drop-down menu on which you can select whether to add an internal or an external group policy. If you simply click Add, then by default, you create an internal group policy. Clicking Add opens the Add Internal Group Policy dialog box or the Add External Group Policy dialog box, which let you add a new group policy to the list. This dialog box includes three menu sections. Click each menu item to display its parameters. As you move from item to item, ASDM retains your settings. When you have finished setting parameters on all menu sections, click Apply or Cancel. Offers a drop-down menu on which you can select whether to add an internal or an external group policy. If you simply click Add, then by default, you create an internal group policy.
- Edit—Displays the Edit Group Policy dialog box, which lets you modify an existing group policy.
- Delete—Lets you remove a AAA group policy from the list. There is no confirmation or undo.

## Adding or Editing a Remote Access Internal Group Policy, General Attributes

The Add or Edit Group Policy dialog box lets you specify tunneling protocols, filters, connection settings, and servers for the group policy being added or modified. For each of the fields on this window, checking the Inherit check box lets the corresponding setting take its value from the default group policy. Inherit is the default value for all of the attributes on this dialog box.



### Note

The fields most important for the VPN Client appear below the More Options line. You must select IPsec as one of the tunneling protocols unless you are certain that the individual group policy or username from which this group would inherit specifies IPsec as the tunneling protocol.

### Fields

The following attributes appear in the Add or Edit Internal Group Policy > General dialog box. They apply to SSL VPN and IPsec sessions, or clientless SSL VPN sessions. Thus, several are present for one type of session, but not the other.

- Name—Specifies the name of this group policy. For the Edit function, this field is read-only.
- Banner—Specifies the banner text to present to users at login. The length can be up to 491 characters. There is no default value.
- Address Pools—(Network (Client) Access only) Specifies the name of one or more address pools to use for this group policy. You configure the address pools by selecting Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools.
- Select—(Network (Client) Access only) Opens the Select Address Pools window, which shows the pool name, starting and ending addresses, and subnet mask of address pools available for client address assignment and lets you select, add, edit, delete, and assign entries from that list.
- More Options—Displays additional configurable options for this group policy.
- Tunneling Protocols—Specifies the tunneling protocols that this group can use. Users can use only the selected protocols. The choices are as follows:
  - Clientless SSL VPN—Specifies the use of VPN via SSL/TLS, which uses a web browser to establish a secure remote-access tunnel to a security appliance; requires neither a software nor hardware client. Clientless SSL VPN can provide easy access to a broad range of enterprise resources, including corporate websites, web-enabled applications, NT/AD file share (web-enabled), e-mail, and other TCP-based applications from almost any computer that can reach HTTPS Internet sites.
  - SSL VPN Client—Specifies the use of the Cisco AnyConnect VPN client or the legacy SSL VPN client.
  - IPsec—IP Security Protocol. Regarded as the most secure protocol, IPsec provides the most complete architecture for VPN tunnels. Both site-to-site (peer-to-peer) connections and client-to-LAN connections can use IPsec.
  - L2TP over IPsec—Allows remote users with VPN clients provided with several common PC and mobile PC operating systems to establish secure connections over the public IP network to the security appliance and private corporate networks. L2TP uses PPP over UDP (port 1701) to tunnel the data. The security appliance must be configured for IPsec transport mode.



### Note

If you do not select a protocol, an error message appears.

- **Filter**—(Network (Client) Access only) Specifies which access control list to use, or whether to inherit the value from the group policy. Filters consist of rules that determine whether to allow or reject tunneled data packets coming through the security appliance, based on criteria such as source address, destination address, and protocol. To configure filters and rules, see the Group Policy window.
- **Web ACL**—(Clientless SSL VPN only) Select an access control list (ACL) from the drop-down list if you want to filter traffic. Click **Manage** next to the list if you want to view, modify, add, or remove ACLs before making a selection.
- **Manage**—Displays the ACL Manager window, with which you can add, edit, and delete Access Control Lists (ACLs) and Extended Access Control Lists (ACEs). For more information about the ACL Manager, see the online Help for that window.
- **NAC Policy**—Selects the name of a Network Admission Control policy to apply to this group policy. You can assign an optional NAC policy to each group policy. The default value is --None--.
- **Manage**—Opens the Configure NAC Policy dialog box. After configuring one or more NAC policies, the NAC policy names appear as options in the drop-down list next to the NAC Policy attribute.
- **Access Hours**—Selects the name of an existing access hours policy, if any, applied to this user or create a new access hours policy. The default value is **Inherit**, or, if the **Inherit** check box is not selected, the default value is --Unrestricted--.
- **Manage**—Opens the Browse Time Range dialog box, on which you can add, edit, or delete a time range.
- **Simultaneous Logins**—Specifies the maximum number of simultaneous logins allowed for this user. The default value is 3. The minimum value is 0, which disables login and prevents user access.



---

**Note** While there is no maximum limit, allowing several simultaneous connections might compromise security and affect performance.

---

- **Restrict Access to VLAN**—(Optional) Also called “VLAN mapping,” this parameter specifies the egress VLAN interface for sessions to which this group policy applies. The security appliance forwards all traffic on this group to the selected VLAN. Use this attribute to assign a VLAN to the group policy to simplify access control. Assigning a value to this attribute is an alternative to using ACLs to filter traffic on a session. In addition to the default value (Unrestricted), the drop-down list shows only the VLANs that are configured on this security appliance.



---

**Note** This feature works for HTTP connections, but not for FTP and CIFS.

---

- **Maximum Connect Time**—If the **Inherit** check box is not selected, this parameter specifies the maximum user connection time in minutes. At the end of this time, the system terminates the connection. The minimum is 1 minute, and the maximum is 35791394 minutes (over 4000 years). To allow unlimited connection time, select **Unlimited** (the default).
- **Idle Timeout**—If the **Inherit** check box is not selected, this parameter specifies this user's idle timeout period in minutes. If there is no communication activity on the user's connection in this period, the system terminates the connection. The minimum time is 1 minute, and the maximum time is 10080 minutes. The default is 30 minutes. To allow unlimited connection time, select **Unlimited**. This value does not apply to Clientless SSL VPN users.

- On smart card removal—With the default option, Disconnect, the client tears down the connection if the smart card used for authentication is removed. Click Keep the connection if you do not want to require users to keep their smart cards in the computer for the duration of the connection.

## Configuring Advanced IPsec Client Parameters

The Add or Edit Group Policy > Advanced > IPsec Client dialog box lets you specify tunneling protocols, filters, connection settings, and servers for the group policy being added or modified.

### Fields

- Re-Authentication on IKE Re-key—Enables or disables reauthentication when IKE re-key occurs, unless the Inherit check box is selected. The user has 30 seconds to enter credentials, and up to three attempts before the SA expires at approximately two minutes and the tunnel terminates.
- Enable extended reauth-on-rekey to allow entry of authentication credentials until SA expiry—Allow users the time to reenter authentication credentials until the maximum lifetime of the configured SA.
- IP Compression—Enables or disables IP Compression, unless the Inherit check box is selected.
- Perfect Forward Secrecy—Enables or disables perfect forward secrecy (PFS), unless the Inherit check box is selected. PFS ensures that the key for a given IPsec SA was not derived from any other secret (like some other keys). In other words, if someone were to break a key, PFS ensures that the attacker would not be able to derive any other key. If PFS were not enabled, someone could hypothetically break the IKE SA secret key, copy all the IPsec protected data, and then use knowledge of the IKE SA secret to compromise the IPsec SAs set up by this IKE SA. With PFS, breaking IKE would not give an attacker immediate access to IPsec. The attacker would have to break each IPsec SA individually.
- Store Password on Client System—Enables or disables storing the password on the client system.



### Caution

---

Storing the password on a client system can constitute a potential security risk.

---

- IPsec over UDP—Enables or disables using IPsec over UDP.
- IPsec over UDP Port—Specifies the UDP port to use for IPsec over UDP.
- Tunnel Group Lock—Enables locking the tunnel group you select from the list, unless the Inherit check box or the value None is selected.
- IPsec Backup Servers—Activates the Server Configuration and Server IP Addresses fields, so you can specify the UDP backup servers to use if these values are not inherited.
  - Server Configuration—Lists the server configuration options to use as an IPsec backup server. The available options are: Keep Client Configuration (the default), Use the Backup Servers Below, and Clear Client Configuration.
  - Server Addresses (space delimited)—Specifies the IP addresses of the IPsec backup servers. This field is available only when the value of the Server Configuration selection is Use the Backup Servers Below.

## Configuring Client Access Rules

The Add or Edit Group Policy > Advanced > IPsec Client > Client Access Rules dialog box lets you permit or deny access by certain types and versions of VPN Clients. If you do not define any rules, the security appliance permits all client types. If a client matches none of the rules, the security appliance denies the connection. If you define a deny rule, you must also define at least one permit rule, or the security appliance denies all connections for the group policy being added or modified.

## Adding or Editing Client Access Rules

The Add or Edit Client Access Rule dialog box adds a new client access rule for an IPsec group policy or modifies an existing rule. The fields on this dialog box relate to various types of VPN clients, so be aware that not all of the possible values are valid for the IPsec VPN Client.

### Fields

- Priority—Shows the priority for this rule.
- Action—Specifies whether this rule permits or denies access.
- VPN Client Type—Specifies the type of VPN client to which this rule applies, software or hardware, and for software clients, all Windows clients or a subset. Some common values for VPN Client Type include VPN 3002, PIX, Linux, \* (matches all client types), and WinNT (matches Windows NT, Windows 2000, Windows XP, and Windows Vista). If you choose \*, do not configure individual Windows types such as Windows XP.
- VPN Client Version—Specifies the version or versions of the VPN client to which this rule applies. This box contains a comma-separated list of software or firmware images appropriate for this client.
- The following caveats apply:
  - You must specify the software version for this client. You can specify \* to match any version.
  - Your entries must match exactly those on the URL for the VPN client, or the TFTP server for the VPN 3002.
  - The TFTP server for distributing the hardware client image must be a robust TFTP server.
  - If the client is already running a software version on the list, it does not need a software update. If the client is not running a software version on the list, an update is in order.
  - A VPN Client user must download an appropriate software version from the listed URL.
  - The VPN 3002 hardware client software is automatically updated via TFTP.

## Configuring Client Firewall Parameters

The Add or Edit Group Policy > Advanced > IPsec Client > Client Firewall dialog box lets you set personal firewall policies for VPN Clients for the group policy being added or modified. The security appliance pushes this firewall policy to the VPN client during connection setup negotiation. If you have users in this group who do not yet have a firewall, choose “Firewall Optional” in the Firewall Setting field.



### Note

Only VPN clients running Microsoft Windows can use these firewall features. These features are currently not available to hardware clients or other (non-Windows) software clients.

A firewall isolates and protects a computer from the Internet by inspecting each inbound and outbound individual packet of data to determine whether to allow or drop it. Firewalls provide extra security if remote users in a group have split tunneling configured. In this case, the firewall protects the user's PC, and thereby the corporate network, from intrusions by way of the Internet or the user's local LAN. Remote users connecting to the security appliance with the VPN client can choose the appropriate firewall option.

In the first scenario, a remote user has a personal firewall installed on the PC. The VPN client enforces firewall policy defined on the local firewall, and it monitors that firewall to make sure it is running. If the firewall stops running, the VPN client drops the connection to the security appliance. (This firewall enforcement mechanism is called Are You There (AYT), because the VPN client monitors the firewall by sending it periodic “are you there?” messages; if no reply comes, the VPN client knows the firewall is down and terminates its connection to the security appliance.) The network administrator might configure these PC firewalls originally, but with this approach, each user can customize his or her own configuration.

In the second scenario, you might prefer to enforce a centralized firewall policy for personal firewalls on VPN client PCs. A common example would be to block Internet traffic to remote PCs in a group using split tunneling. This approach protects the PCs, and therefore the central site, from intrusions from the Internet while tunnels are established. This firewall scenario is called push policy or Central Protection Policy (CPP). On the security appliance, you create a set of traffic management rules to enforce on the VPN client, associate those rules with a filter, and designate that filter as the firewall policy. The security appliance pushes this policy down to the VPN client. The VPN client then in turn passes the policy to the local firewall, which enforces it.

## Fields

- **Inherit**—Determines whether the group policy obtains its client firewall setting from the default group policy. This option is the default setting. When set, it overrides the remaining attributes in this tab and dims their names.
- **Firewall Setting**—Lists whether a firewall exists, and if so, whether it is required or optional. If you select No Firewall (the default), none of the remaining fields on this window are active. If you want users in this group to be firewall-protected, select either the Firewall Required or Firewall Optional setting.

If you select Firewall Required, all users in this group must use the designated firewall. The security appliance drops any session that attempts to connect without the designated, supported firewall installed and running. In this case, the security appliance notifies the VPN client that its firewall configuration does not match.



**Note** If you require a firewall for a group, make sure the group does not include any clients other than Windows VPN clients. Any other clients in the group (including ASA 5505 in client mode and VPN 3002 hardware clients) are unable to connect.

If you have remote users in this group who do not yet have firewall capacity, choose Firewall Optional. The Firewall Optional setting allows all the users in the group to connect. Those who have a firewall can use it; users that connect without a firewall receive a warning message. This setting is useful if you are creating a group in which some users have firewall support and others do not—for example, you may have a group that is in gradual transition, in which some members have set up firewall capacity and others have not yet done so.

- Firewall Type—Lists firewalls from several vendors, including Cisco. If you select Custom Firewall, the fields under Custom Firewall become active. The firewall you designate must correlate with the firewall policies available. The specific firewall you configure determines which firewall policy options are supported.
- Custom Firewall—Specifies the vendor ID, Product ID and description for the custom firewall.
  - Vendor ID—Specifies the vendor of the custom firewall for this group policy.
  - Product ID—Specifies the product or model name of the custom firewall being configured for this group policy.
  - Description—(Optional) Describes the custom firewall.
- Firewall Policy—Specifies the type and source for the custom firewall policy.
  - Policy defined by remote firewall (AYT)—Specifies that the firewall policy is defined by the remote firewall (Are You There). Policy defined by remote firewall (AYT) means that remote users in this group have firewalls located on their PCs. The local firewall enforces the firewall policy on the VPN client. The security appliance allows VPN clients in this group to connect only if they have the designated firewall installed and running. If the designated firewall is not running, the connection fails. Once the connection is established, the VPN client polls the firewall every 30 seconds to make sure that it is still running. If the firewall stops running, the VPN client ends the session.
  - Policy pushed (CPP)—Specifies that the policy is pushed from the peer. If you select this option, the Inbound Traffic Policy and Outbound Traffic Policy lists and the Manage button become active. The security appliance enforces on the VPN clients in this group the traffic management rules defined by the filter you choose from the Policy Pushed (CPP) drop-down menu. The choices available on the menu are filters defined on this security appliance, including the default filters. Keep in mind that the security appliance pushes these rules down to the VPN client, so you should create and define these rules relative to the VPN client, not the security appliance. For example, “in” and “out” refer to traffic coming into the VPN client or going outbound from the VPN client. If the VPN client also has a local firewall, the policy pushed from the security appliance works with the policy of the local firewall. Any packet that is blocked by the rules of either firewall is dropped.
  - Inbound Traffic Policy—Lists the available push policies for inbound traffic.
  - Outbound Traffic Policy—Lists the available push policies for outbound traffic.
- Manage—Displays the ACL Manager window, on which you can configure Access Control Lists (ACLs).

## Configuring Hardware Client Parameters

You do not configure these parameters for the VPN Client. Configure the hardware client parameters on the Add or Edit Group Policy > Advanced > IPsec Client > Hardware Client dialog box only if you are configuring a hardware client such as the ASA 5505 used as a hardware client.

