CHAPTER 2

Configuring AnyConnect Features Using ASDM

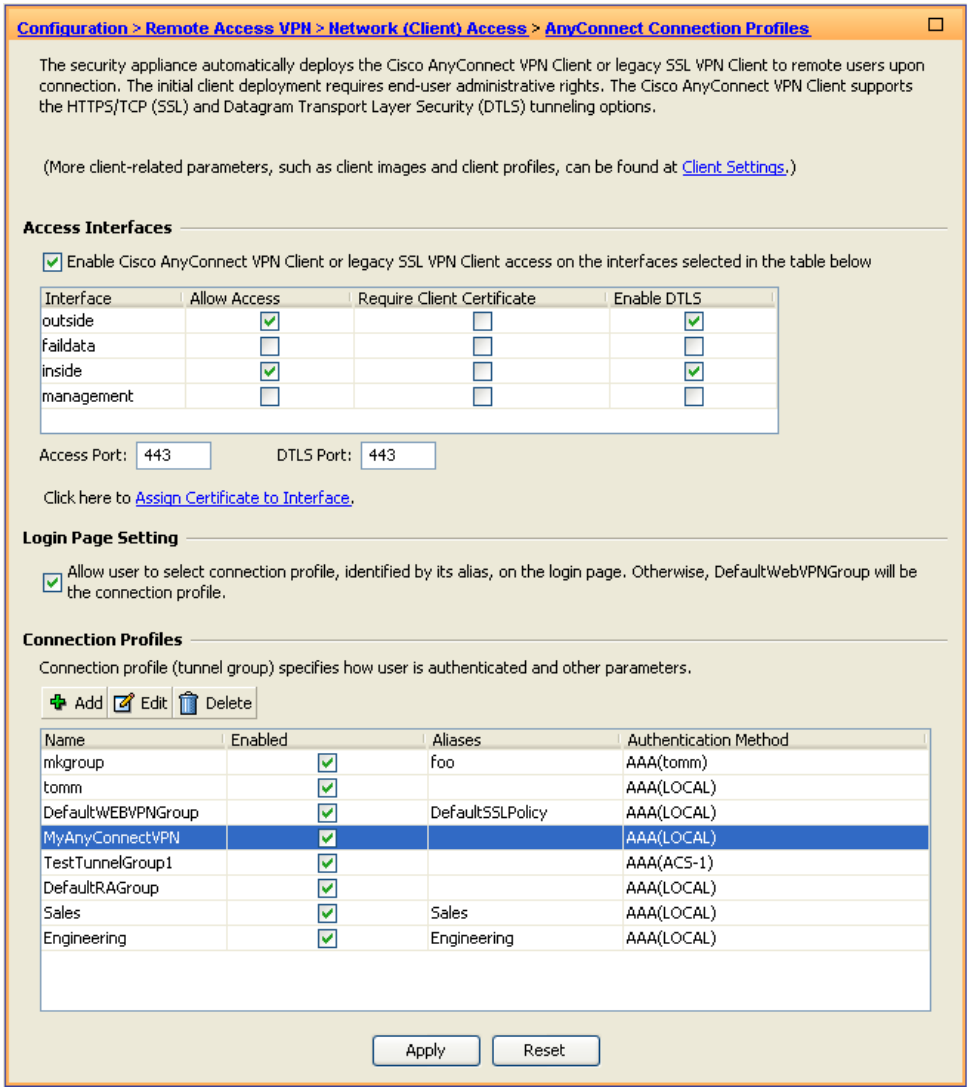
The security appliance automatically deploys the Cisco AnyConnect VPN client to remote users upon connection. The initial client deployment requires end-user administrative rights. The AnyConnect client supports the HTTPS/TCP (SSL) and Datagram Transport Layer Settings (DTLS) tunneling options. This chapter describes how to use ASDM to configure AnyConnect features.

You configure the AnyConnect client features on the security appliance, as described in the following sections:

Enabling the SSL VPN Client Protocol

The AnyConnect client uses the SSL VPN protocol, therefore you must enable the SSL VPN Client protocol as part of the configuration process. To do this, select Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles. The AnyConnect Connection Profiles window appears (Figure 2-1).

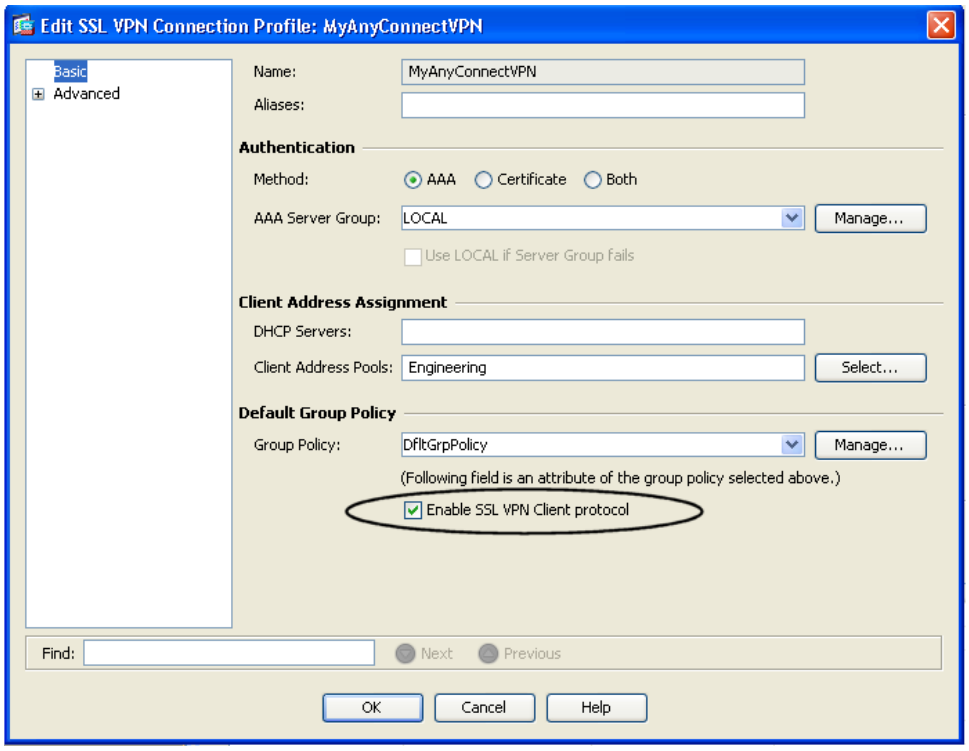
Figure 2-1 AnyConnect Connection Profiles Window



In the Access Interfaces area, select the check box to enable Cisco AnyConnect VPN Client access on the interfaces selected in the table.

In the Connection Profiles area of the window, select the profile you want to configure, then click Add or Edit. The Add or Edit SSL VPN Connection Profile dialog box appears, with Basic selected in the navigation panel (Figure 2-2). If you are using the Default Group Policy, select the check box for Enable SSL VPN Client Protocol and click OK.

Figure 2-2 Edit SSL VPN Connection Profile Dialog Box



Configuring the Login Page Setting

To allow the user to select a connection profile, identified by its alias, on the login page, select the check box in the Login Page Setting area of the AnyConnect Connection Profiles window (Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles). If you do not select this feature, the AnyConnect client uses the DefaultWebVPNGroup profile as the connection profile.

To specify an alias for a connection profile, first select the profile in the AnyConnect Profile window and click Add or Edit, as above. On the Add of Edit SSL VPN Connection profile dialog box, select Advanced > SSL VPN and in the Connection Aliases area, click Add. The Add Connection Alias dialog box appears. Specify an alias to use for this connection profile, and click Enabled, then OK. The alias you specify appears in the Aliases field of the AnyConnect Connection Profiles window.

Enabling Datagram Transport Layer Security (DTLS) with AnyConnect (SSL) Connections

Datagram Transport Layer Security avoids latency and bandwidth problems associated with some SSL-only connections, including AnyConnect connections, and improves the performance of real-time applications that are sensitive to packet delays. DTLS is a standards-based SSL protocol that provides a low-latency data path using UDP. For detailed information about DTLS, see RFC 4347 (http://www.ietf.org/rfc/rfc4347.txt).

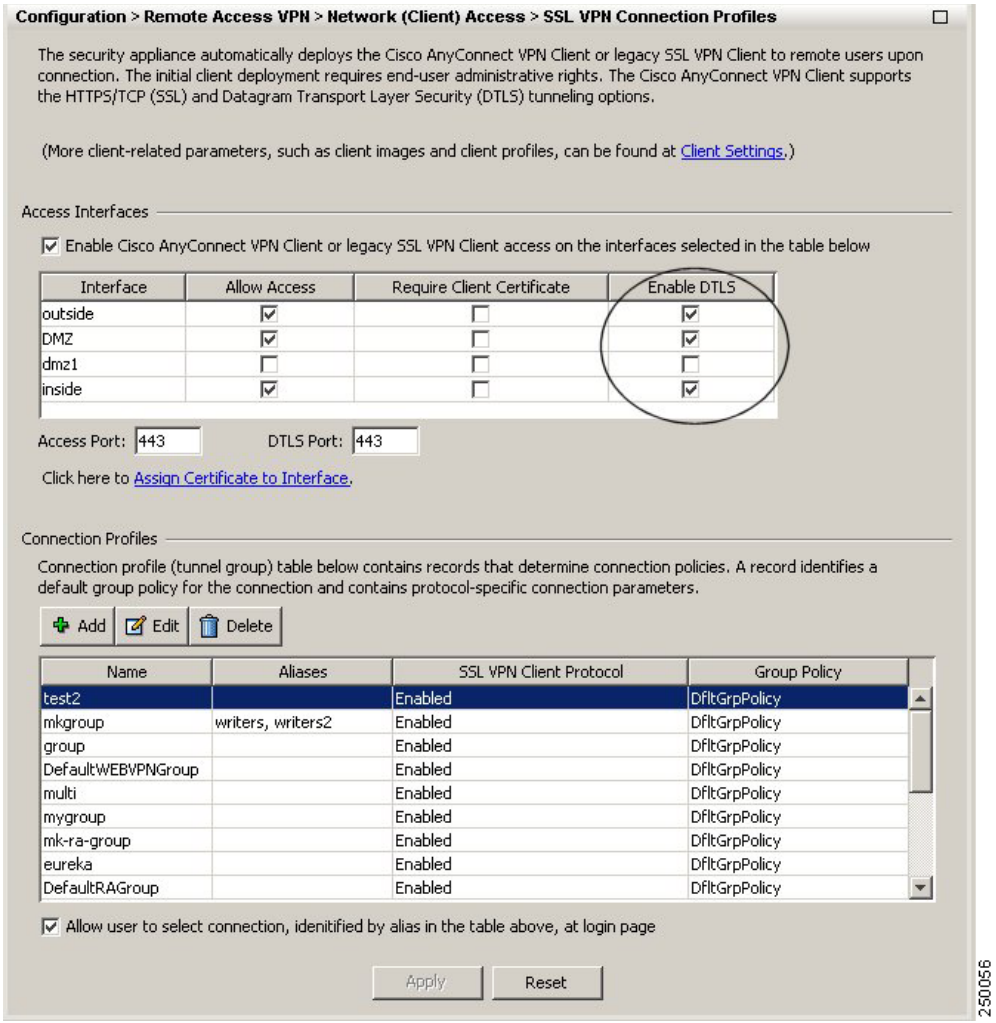
Datagram Transport Layer Security (DTLS) allows the AnyConnect client establishing an SSL VPN connection to use two simultaneous tunnels—an SSL tunnel and a DTLS tunnel. Using DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays.

If you do not enable DTLS, AnyConnect/SSL VPN connections connect with an SSL VPN tunnel only.

You cannot enable DTLS globally with ASDM. The following section describes how to enable DTLS for any specific interface.

To enable DTLS for a specific interface, select Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN Connection profiles. The SSL VPN Connection Profiles dialog box opens (Figure 2-3).

Figure 2-3 Enable DTLS Check Box



To enable DTLS on an interface, select the check box in its row. To specify a separate UDP port to use for AnyConnect, enter the port number in the UDP Port field. The default value is port 443.

Configuring DTLS

If DTLS is configured and UDP is interrupted, the remote user's connection automatically falls back from DTLS to TLS. The default is enabled; however, DTLS is not enabled by default on any individual interface.

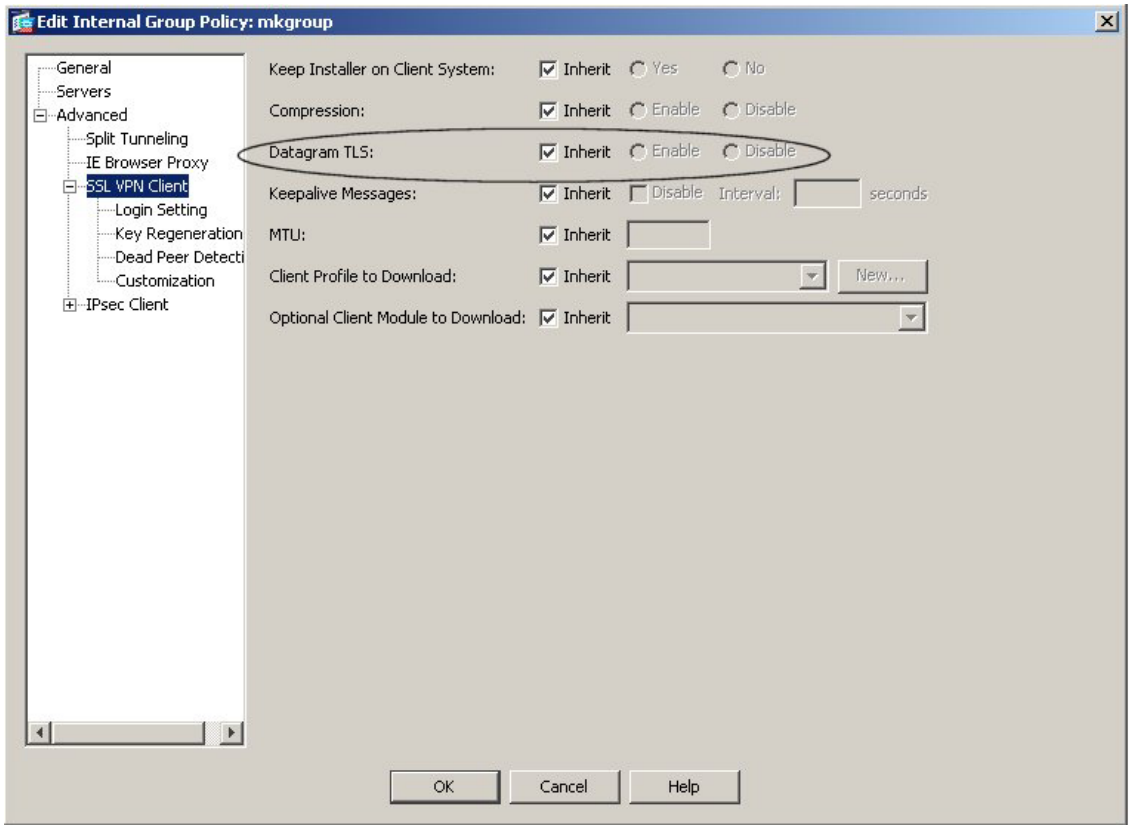
Enabling DTLS allows the AnyConnect client establishing an AnyConnect VPN connection to use two simultaneous tunnels—an SSL tunnel and a DTLS tunnel. Using DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays.

If you do not enable DTLS, AnyConnect client users establishing SSL VPN connections connect only with an SSL VPN tunnel. To enable DTLS, use the Datagram TLS setting in either Group Policy or Username. The paths to this setting are:

- Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit > Add or Edit Internal Group Policy > Advanced > SSL VPN Client
- Configuration > Remote Access VPN > Network (Client) Access > AAA Setup > Local Users > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client
- Device Management > Users/AAA > User Accounts > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client

Figure 2-4 shows an example of configuring the DTLS setting for an internal group policy.

Figure 2-4 Enabling or Disabling DTLS



Note When using the AnyConnect client with DTLS on security appliance, Dead Peer Detection must be enabled in the group policy on the security appliance to allow the AnyConnect client to fall back to TLS, if necessary. Fallback to TLS occurs if the AnyConnect client cannot send data over the UPD/DTLS session, and the DPD mechanism is necessary for fallback to occur.

Prompting Remote Users

To enable the security appliance to prompt remote AnyConnect VPN client users to download the client, select Configuration > Device Management > Users/AAA > User Accounts > Add or Edit. The Add or Edit dialog box appears. In the navigation panel on the left, select VPN Policy > SSL VPN Client > Login Setting (Figure 2-5).

Figure 2-5 Edit User Account Dialog Box for Prompt Setting

Deselect the Inherit check box, if necessary, and in the Post Login Setting area, select the option Prompt user to choose. To disable this option, select Do not prompt user to choose.

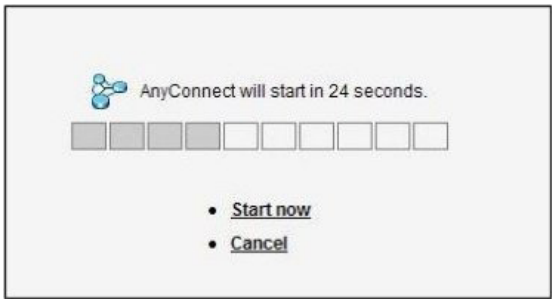
When you enable the prompting option, another field becomes available, asking you to specify the number of seconds the user has to choose before the Default Post Login selection takes effect.

Select the Default Post Login selection to specify the action that the AnyConnect client takes if the user does not make a selection before the timer specified in the prompting option expires. The options are:

- Go to Clientless SSL VPN Portal—Immediately displays the portal page for Clientless SSL VPN. The user can still invoke the AnyConnect client from the portal by clicking Start AnyConnect Client.
- Download SSL VPN Client—Immediately starts downloading the AnyConnect client to the remote user's PC.

Figure 2-6 shows the prompt displayed to remote users when either the default svc timeout value or the default webvpn timeout value is configured (in this case, the timeout was set to 35 seconds):

Figure 2-6 Prompt Displayed to Remote Users for SSL VPN Client Download



Enabling Modules for Additional AnyConnect Features

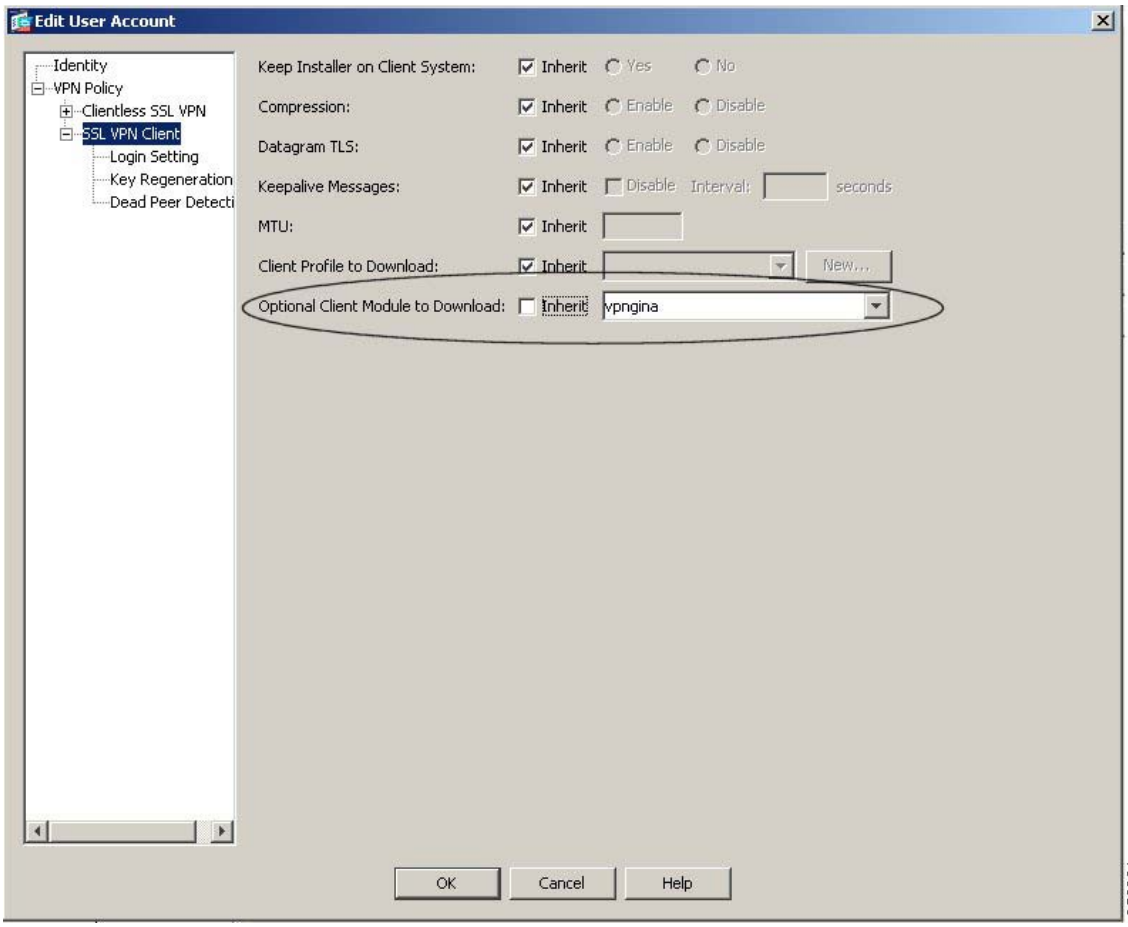
As new features are released for the AnyConnect client, you must update the AnyConnect clients of your remote users for them to use the new features. To minimize download time, the AnyConnect client requests downloads (from the security appliance) only of modules that it needs for each feature that it supports.

To enable new features, you must specify the new module names as part of the group-policy or username configuration. Possible paths to the dialog box where you can specify these modules are:

- Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit > Add or Edit Internal Group Policy > Advanced > SSL VPN Client
- Configuration > Remote Access VPN > Network (Client) Access > AAA Setup > Local Users > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client
- Device management > Users/AAA > User Accounts > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client.

Specify the module name—for example, **vpngina** for the Start Before Logon feature—in the Optional Client Module to Download field. Separate multiple strings with commas. Figure 2-7 shows an example.

Figure 2-7 Optional Client Module to Download



In the case of Start Before Logon, you must also enable the feature in the XML profile file. See Configuring Profile Attributes, page 4-10 for details.

Note For Release 2.3, you can select **vpngina** from the drop-down list or manually enter the keyword into the field. This enables Start Before Logon for Windows Vista, Windows XP, and Windows 2000. If you have downloaded the Beta software for DART (Diagnostic Analysis and Reporting Tool), you can also enter the keyword **dart** into this field, either alone or in combination with **vpngina**, as long as these values are separated by a comma.

Configuring, Enabling, and Using Other AnyConnect Features

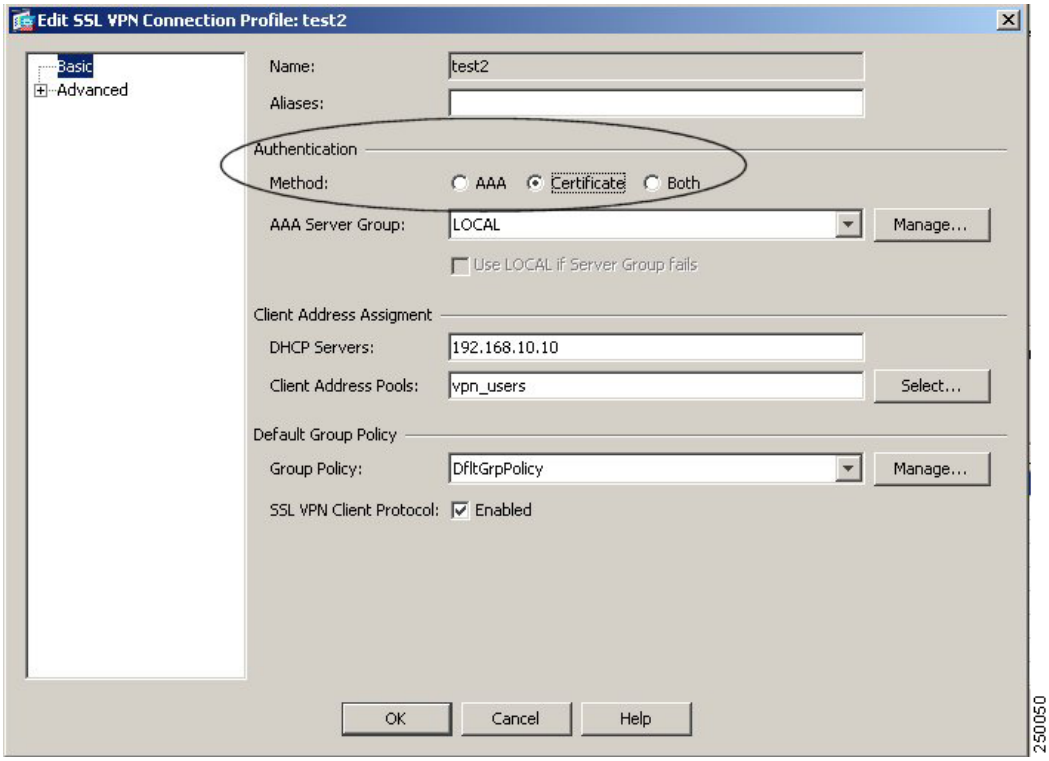
The following sections describe how to configure other AnyConnect features. Some features, such as Secure Desktop and dynamic access policies, do not require that you specifically configure the AnyConnect client to interact with that feature. Rather, all configuration for those features occurs on the security appliance or within the respective software packages.

Configuring Certificate-only Authentication

You can specify whether you want users to authenticate using AAA with a username and password or using a digital certificate (or both). When you configure certificate-only authentication, users can connect with a digital certificate and are not required to provide a user ID and password.

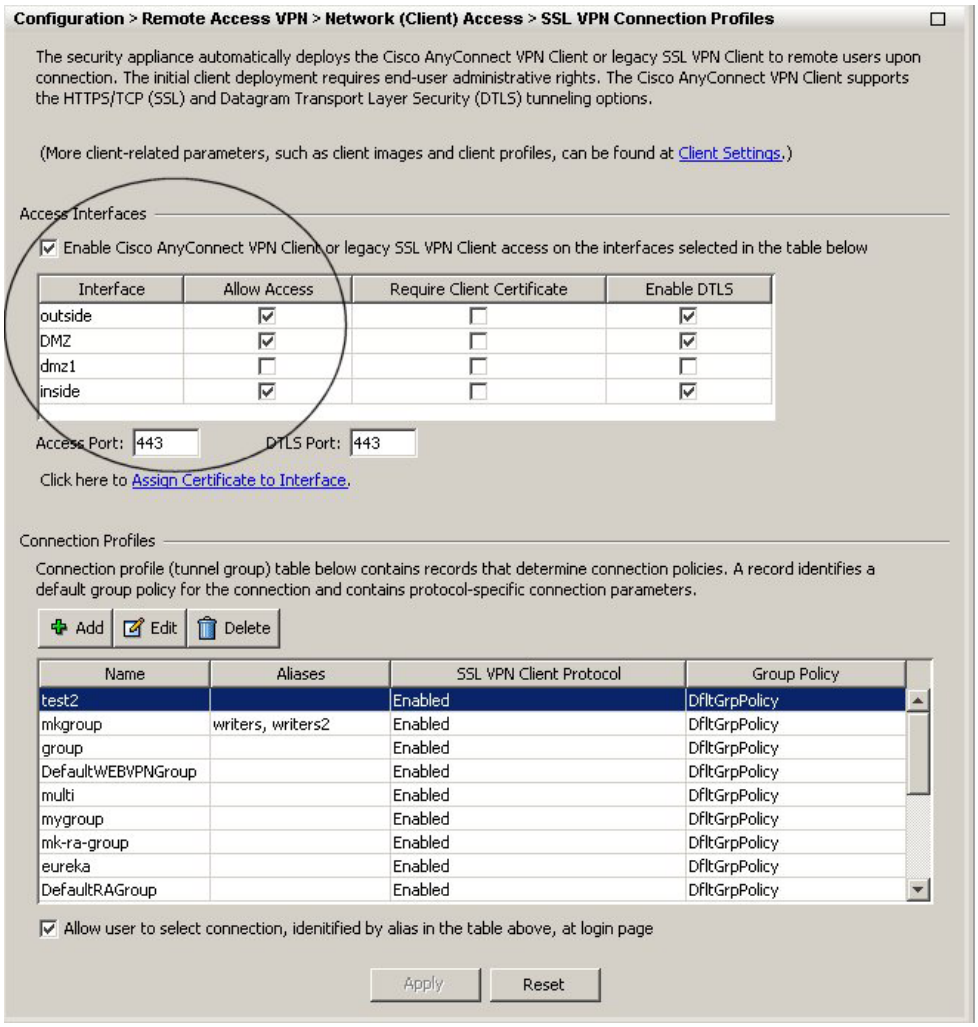
To configure certificate-only authentication using ASDM, select Configuration > Remote Access > Network (Client) Access > SSL VPN Connection Profiles, and in the Connection Profiles area, select Add or Edit. This displays the Add or Edit SSL VPN Connect Profile dialog box with the Basic option selected. In the Authentication area, select only Certificate as the Method.

Figure 2-8 Configuring Certificate-Only Authentication, Edit SSL VPN Dialog Box



To make this feature take effect, you must also enable AnyConnect client access on particular interfaces and ports, as needed. To do this, select Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles. The SSL VPN Connection Profiles dialog box (Figure 2-9) appears.

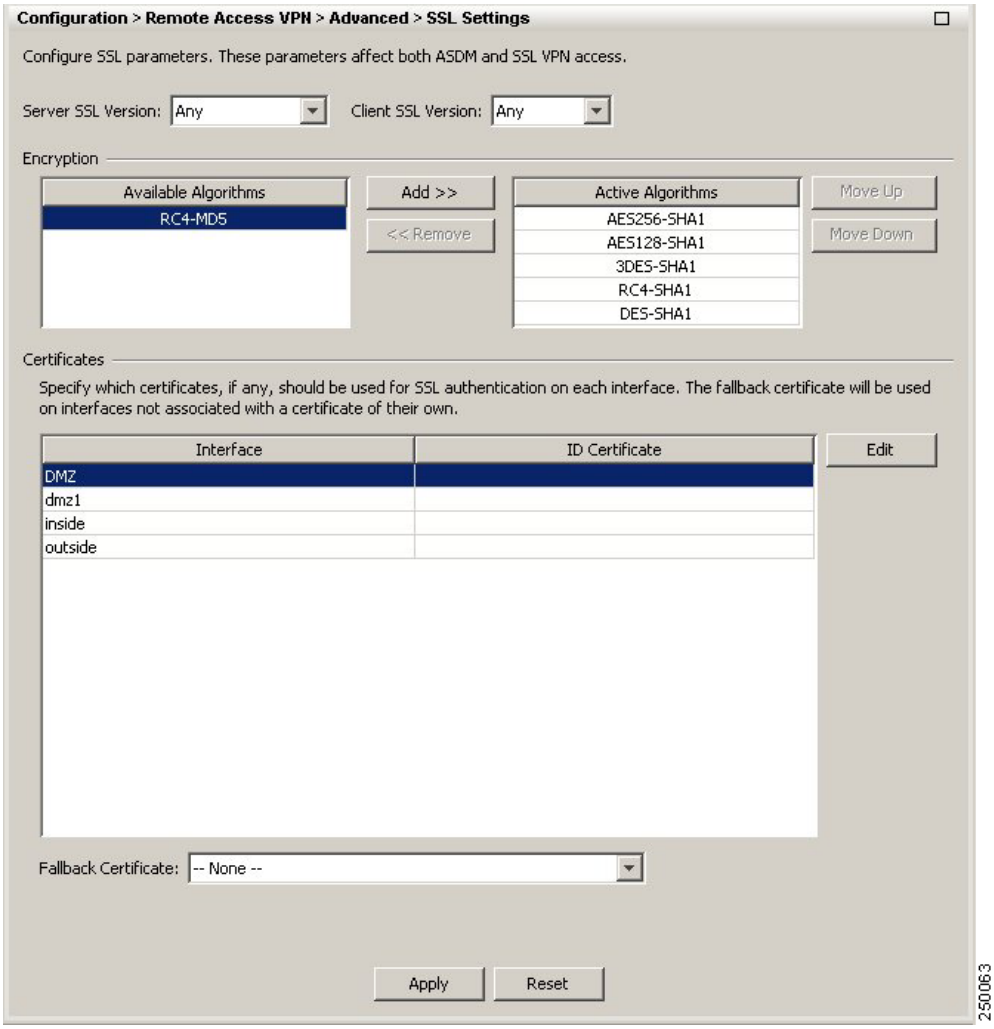
Figure 2-9 SSL VPN Connection Profiles Dialog Box



In the Access Interfaces area, select the check box Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interfaces selected in the table below. Then select the check boxes for the interfaces on which you want to enable access. Specify the Access Port. The default access port is 443.

If you want to assign a specific certificate to an interface, click Assign Certificate to Interface. This opens the SSL Settings dialog box (Figure 2-10).

Figure 2-10 SSL Settings Dialog Box



In the Certificates area, specify which certificates, if any, you want to use for SSL authentication on each interface. If you do not specify a certificate for a particular interface, the fallback certificate will be used. In the Fallback Certificate field, select a certificate from the drop-down list. The default is --None--.

Using Compression

On low-bandwidth connections, compression increases the communications performance between the security appliance and the client by reducing the size of the packets being transferred. By default, compression for all SSL VPN connections is enabled on the security appliance, both at the global level and for specific groups or users. For broadband connections, compression might result in poorer performance.

By default, if you have not changed the compression setting globally, compression is enabled. You can configure compression globally using the CLI command **compression svc** command from global configuration mode.

Note The AnyConnect client for Windows Mobile does not support compression.

Changing Compression Globally

To change the global compression settings, use the **compression svc** command from global configuration mode:

compression svc

no compression svc

To remove the command from the configuration, use the **no** form of the command.

In the following example, compression is disabled for all SSL VPN connections globally:

```
hostname(config)# no compression svc
```

Changing Compression for Groups and Users

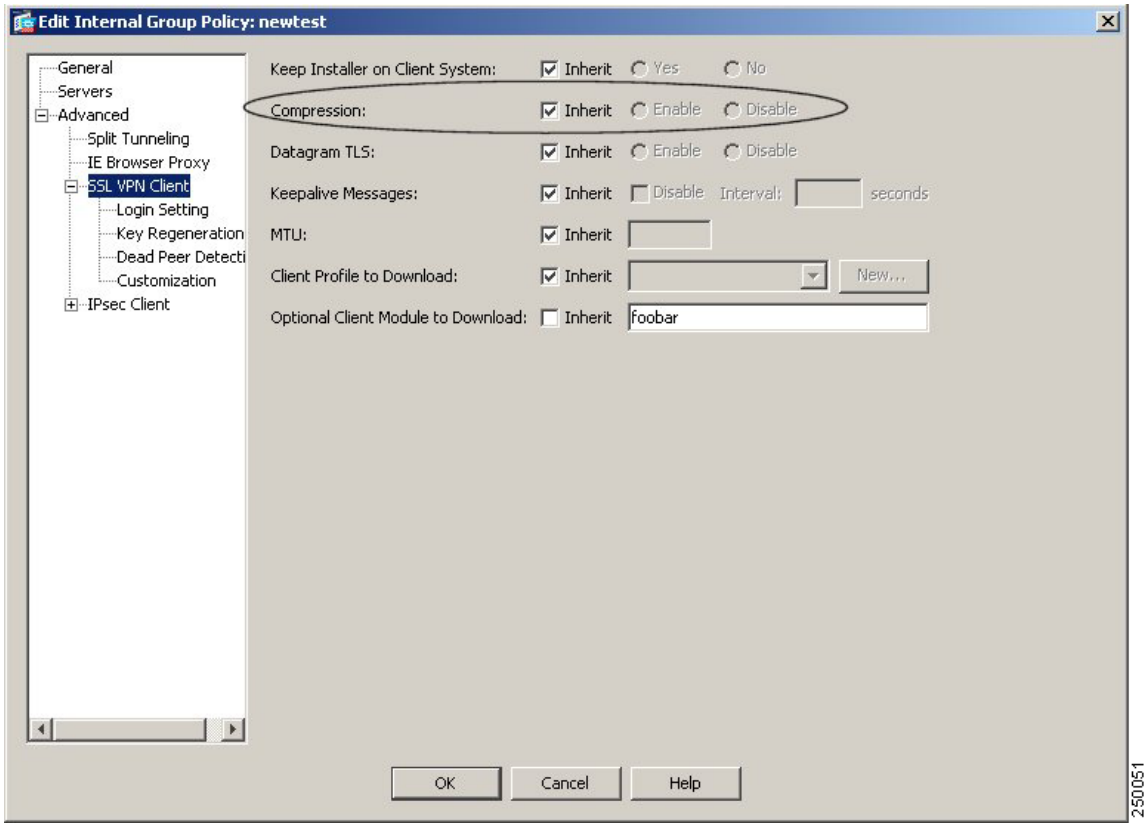
You can also configure compression for specific groups or users using ASDM with the **svc compression** command in group-policy and username webvpn modes. The global setting overrides the group-policy and username settings.

To change compression for a specific group or user, use the Compression setting in either Group Policy or Username. You can get to this setting through any of the following paths:

- Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit > Add or Edit Internal Group Policy > Advanced > SSL VPN Client
- Configuration > Remote Access VPN > Network (Client) Access > AAA Setup > Local Users > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client
- Device Management > Users/AAA > User Accounts > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client

Figure 2-11 shows an example of configuring the compression setting for an internal group policy.

Figure 2-11 Compression Setting



By default, for groups and users, SSL compression is set to Inherit. If you deselect Inherit, the default is enabled (equivalent to *deflate* in the CLI).

Note For compression to work, it must be enabled both globally (by the **compression svc** command configured from global configuration mode) and for the specific group policy or username. If *either* is set to disable (or to the **none** or the **no** form of the command), compression is disabled.

Enabling AnyConnect Keepalives

You can adjust the frequency of keepalive messages to ensure that an AnyConnect client or SSL VPN connection through a proxy, firewall, or NAT device remains open, even if the device limits the time that the connection can be idle. Adjusting the frequency also ensures that the client does not disconnect and reconnect when the remote user is not actively running a socket-based application, such as Microsoft Outlook or Microsoft Internet Explorer.

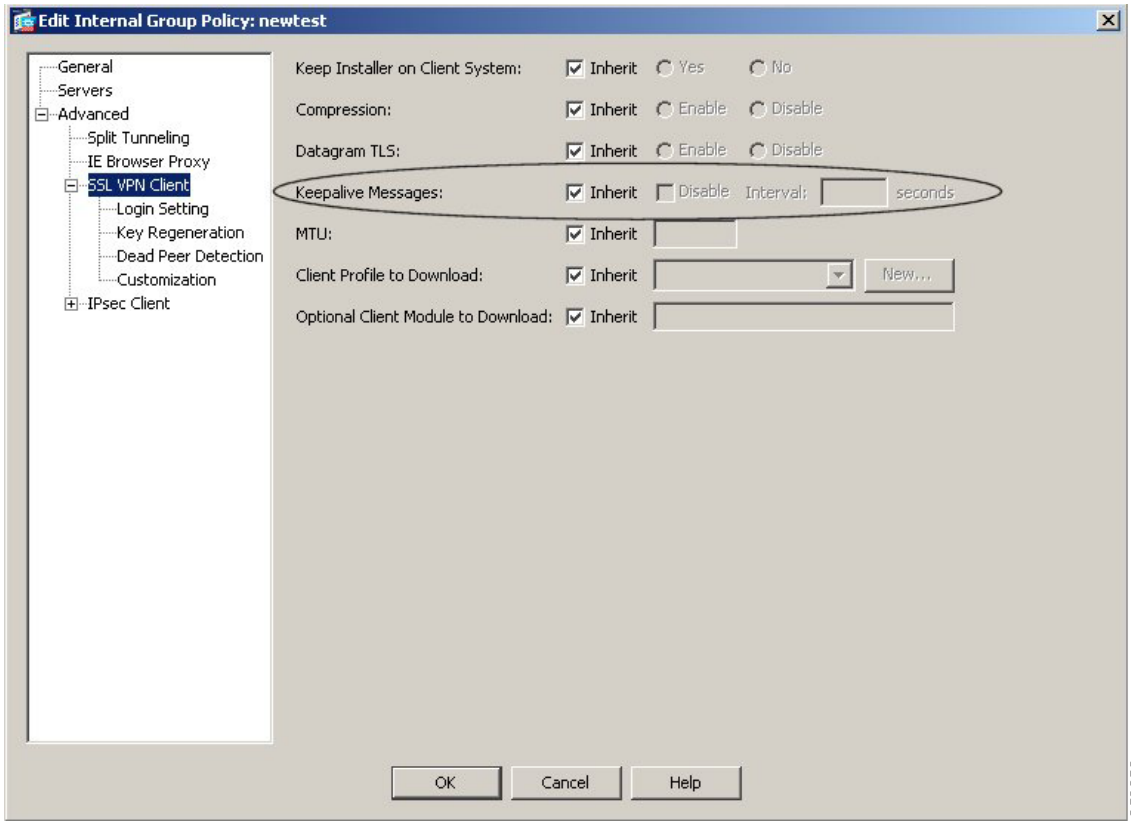
To set the frequency of keepalive messages, use the Keepalive Messages setting in either Group Policy or Username. The paths to this setting are:

- Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit > Add or Edit Internal Group Policy > Advanced > SSL VPN Client
- Configuration > Remote Access VPN > Network (Client) Access > AAA Setup > Local Users > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client

- Device Management > Users/AAA > User Accounts > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client

Figure 2-12 shows an example of configuring the keepalive messages setting for an internal group policy.

Figure 2-12 Configuring Keepalive Messages



Configure the Keepalive Messages field for this attributeby deselecting Inherit and entering a number, from 15 to 600 seconds, in the Interval field to enable and adjust the interval of keepalive messages to ensure that an connection through a proxy, firewall, or NAT device remains open, even if the device limits the time that the connection can be idle. Adjusting the interval also ensures that the client does not disconnect and reconnect when the remote user is not actively running a socket-based application, such as Microsoft Outlook or Microsoft Internet Explorer.

Enabling AnyConnect Rekey

Configuring AnyConnect Rekey specifies that SSL renegotiation takes place during rekey. When the security appliance and the SSL VPN client perform a rekey, they renegotiate the crypto keys and initialization vectors, increasing the security of the connection.

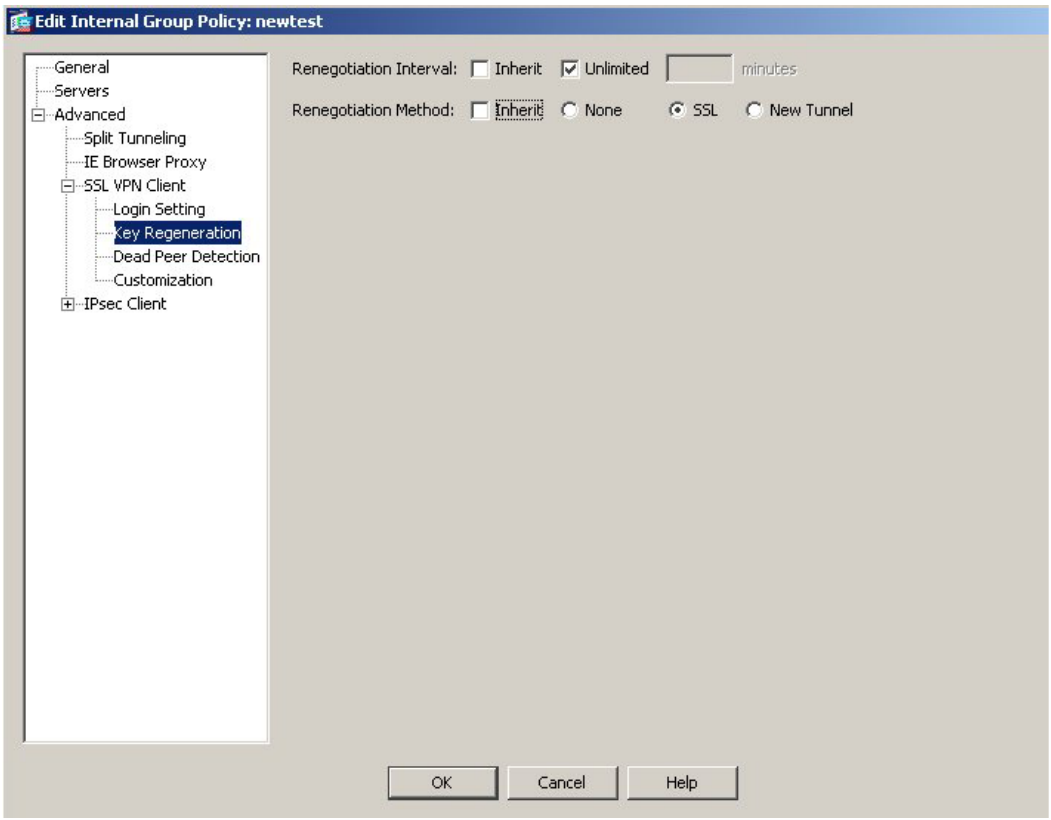
To enable Rekey, use the Key Regeneration dialog box in either Group Policy or Username. The paths to this setting are:

- Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit > Add or Edit Internal Group Policy > Advanced > SSL VPN Client > Key Regeneration

- Configuration > Remote Access VPN > Network (Client) Access > AAA Setup > Local Users > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client > Key Regeneration
- Device Management > Users/AAA > User Accounts > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client > Key Regeneration

Figure 2-13 shows an example of configuring the Rekey setting for an internal group policy.

Figure 2-13 Configuring Rekey Attributes



Key renegotiation occurs when the security appliance and the client perform a rekey and they renegotiate the crypto keys and initialization vectors, increasing the security of the connection. The fields on this dialog box are as follows:

- Renegotiation Interval—Clear the Unlimited check box to specify the number of minutes from the start of the session until the rekey takes place, from 1 to 10080 (1 week).
- Renegotiation Method—Check the None check box to disable rekey, check the SSL check box to specify SSL renegotiation during a rekey, or check the New Tunnel check box to establish a new tunnel during rekey.

Note The security appliance does not currently support inline DTLS rekey. The AnyConnect client, therefore, treats all DTLS rekey events as though they were of the new tunnel method instead of the inline ssl type.

Enabling and Adjusting Dead Peer Detection

Dead Peer Detection (DPD) ensures that the security appliance (gateway) or the client can quickly detect a condition where the peer is not responding, and the connection has failed.

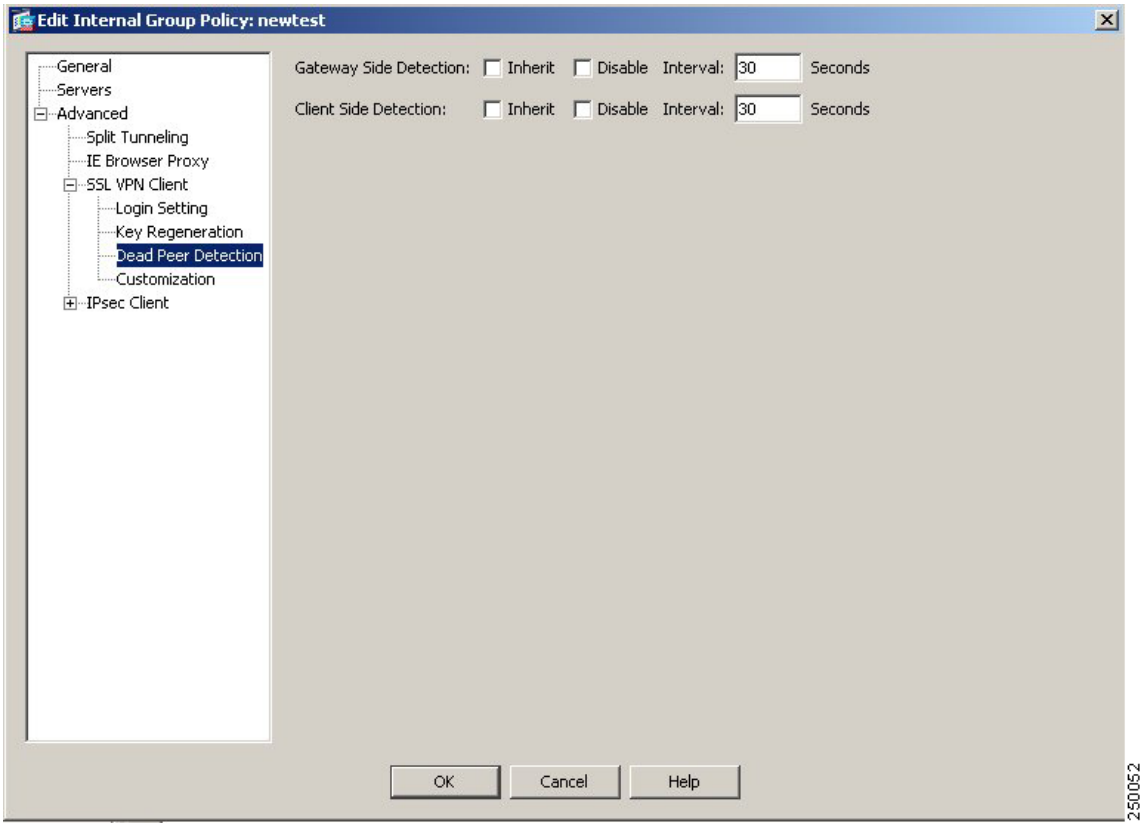
Note When using the AnyConnect client with DTLS on security appliance, Dead Peer Detection must be enabled in the group policy on the security appliance to allow the AnyConnect client to fall back to TLS, if necessary. Fallback to TLS occurs if the AnyConnect client cannot send data over the UPD/DTLS session, and the DPD mechanism is necessary for fallback to occur.

To enable DPD on the security appliance or client for a specific group or user, and to set the frequency with which either the security appliance or client performs dead-peer detection, use the Dead Peer Detection dialog box for either group-policy or username. The paths to this setting are:

- Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit > Add or Edit Internal Group Policy > Advanced > SSL VPN Client > Dead Peer Detection
- Configuration > Remote Access VPN > Network (Client) Access > AAA Setup > Local Users > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client > Dead Peer Detection
- Device Management > Users/AAA > User Accounts > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client > Dead Peer Detection

Figure 2-14 shows an example of configuring the Dead Peer Detection setting for an internal group policy.

Figure 2-14 Enabling or Disabling Dead Peer Detection



In this dialog box, you can set the following attributes:

- Gateway Side Detection—Deselect the Disable check box to specify that dead-peer detection is performed by the *security appliance* (gateway). Enter the interval, from 30 to 3600 seconds, with which the security appliance performs dead-peer detection.
- Client Side Detection—Deselect the Disable check box to specify that dead-peer detection is performed by the *client*. Enter the interval, from 30 to 3600 seconds, with which the client performs dead-peer detection.

Configuring the Dynamic Access Policies Feature of the Security Appliance

On the security appliance, you can configure authorization that addresses the variables of multiple group membership and endpoint security for VPN connections. There is no specific configuration of AnyConnect required to use dynamic access policies. For detailed information about configuring dynamic access policies, see *Cisco ASDM User Guide, Cisco Security Appliance Command Line Configuration Guide,* or *Cisco Security Appliance Command Reference.*

Configuring Cisco Secure Desktop Support

Cisco Secure Desktop validates the security of client computers requesting access to your SSL VPN, helps ensure they remain secure while they are connected, and attempts to remove traces of the session after they disconnect. The Cisco AnyConnect VPN Client supports the Secure Desktop functions of Cisco Secure Desktop for Windows 2000 and Windows XP. There is no specific configuration of AnyConnect required to use Secure Desktop. For detailed information about configuring Cisco Secure Desktop, see the *Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators (Software Release 3.4)*.

Configuring Windows Mobile Support Using ASDM

You configure AnyConnect client Windows Mobile support just as you would any other Windows platform, with the following considerations:

- Windows Mobile connections require a special license, which you install just as you would any other AnyConnect client license. If you do not have this licensed installed, Windows Mobile connections do not work.
- See the latest version of *Release Notes for Cisco AnyConnect VPN Client* for detailed, current information about Windows Mobile device support.
- AnyConnect client Windows Mobile connections do not support compression.
- Windows Mobile connections can use the default profile values, but you can configure a profile that specifies mobile policy device lock parameters. See Configuring Windows Mobile Policy, page 4-22 for details on configuring the Windows Mobile parameters.

Note The AnyConnect client supports Mobile Device Lock on Windows Mobile 5.0, 5.0AKU2, and 6.0, but not on Windows Mobile 6.1.

- If you have configured a profile specifically for Windows Mobile, then under Group Policy, select a client profile to download that has Windows Mobile support enabled. Select Configuration > Remote Access VPN > Network (Client) Access > Group Policies, then click Add or Edit to either add a group policy or edit an existing one. The Add or Edit Group Policy dialog box appears. Select Advanced > SSL VPN Client and specify a client profile to download.

Adding a Security Appliance to the List of Trusted Sites (IE)

To add a security appliance to the list of trusted sites, use Microsoft Internet Explorer and do the following steps.

Note This is required on Windows Vista to use WebLaunch.

Step 1 Go to Tools | Internet Options | Trusted Sites.

The Internet Options window opens.

Step 2 Click the Security tab.

Step 3 Click the Trusted Sites icon.

Step 4 Click Sites.

The Trusted Sites window opens.

Step 5 Type the host name or IP address of the security appliance. Use a wildcard such as https://*.yourcompany.com to allow all ASA 5500s within the yourcompany.com domain to be used to support multiple sites.

Step 6 Click Add.

Step 7 Click OK.

The Trusted Sites window closes.

Step 8 Click OK in the Internet Options window.

Adding a Security Certificate in Response to Browser Alert Windows

This section explains how to install a self-signed certificate as a trusted root certificate on a client in response to the browser alert windows.

In Response to a Microsoft Internet Explorer "Security Alert" Window

The following procedure explains how to install a self-signed certificate as a trusted root certificate on a client in response to a Microsoft Internet Explorer Security Alert window. This window opens when you establish a Microsoft Internet Explorer connection to a security appliance that is not recognized as a trusted site. The upper half of the Security Alert window shows the following text:

```
Information you exchange with this site cannot be viewed or changed by others.
However, there is a problem with the site's security certificate. The security
certificate was issued by a company you have not chosen to trust. View the certificate
to determine whether you want to trust the certifying authority.
```

Install the certificate as a trusted root certificate as follows:

Step 1 Click View Certificate in the Security Alert window.

The Certificate window opens.

Step 2 Click Install Certificate.

The Certificate Import Wizard Welcome opens.

Step 3 Click Next.

The Certificate Import Wizard – Certificate Store window opens.

Step 4 Select "Automatically select the certificate store based on the type of certificate."

Step 5 Click Next.

The Certificate Import Wizard – Completing window opens.

Step 6 Click Finish.

Step 7 Another Security Warning window prompts "Do you want to install this certificate?" Click Yes.

The Certificate Import Wizard window indicates the import is successful.

Step 8 Click OK to close this window.

Step 9 Click OK to close the Certificate window.

Step 10 Click Yes to close the Security Alert window.

The security appliance window opens, signifying the certificate is trusted.

In Response to a Netscape, Mozilla, or Firefox "Certified by an Unknown Authority" Window

The following procedure explains how to install a self-signed certificate as a trusted root certificate on a client in response to a "Web Site Certified by an Unknown Authority" window. This window opens when you establish a Netscape, Mozilla, or Firefox connection to a security appliance that is not recognized as a trusted site. This window shows the following text:

```
Unable to verify the identity of <Hostname_or_IP_address> as a trusted site.
```

Install the certificate as a trusted root certificate as follows:

Step 1 Click the Examine Certificate button in the "Web Site Certified by an Unknown Authority" window.

The Certificate Viewer window opens.

Step 2 Click the "Accept this certificate permanently" option.

Step 3 Click OK.

The security appliance window opens, signifying the certificate is trusted.