CHAPTER 5

Configuring AnyConnect Features Using ASDM

The AnyConnect client includes the following features, which you configure on the security appliance:

- Enabling Datagram Transport Layer Security (DTLS) with AnyConnect (SSL) Connections, page 5-1
- Prompting Remote Users, page 5-4
- Enabling IPv6 VPN Access, page 5-5
- Enabling Modules for Additional AnyConnect Features, page 5-5
- Configuring Certificate-only Authentication, page 5-6
- Using Compression, page 5-9
- Configuring DTLS, page 5-2
- Enabling AnyConnect Keepalives, page 5-11
- Configuring the Dynamic Access Policies Feature of the Security Appliance, page 5-15
- Cisco Secure Desktop Support, page 5-15
- Enabling AnyConnect Rekey, page 5-12
- Enabling and Adjusting Dead Peer Detection, page 5-14

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).

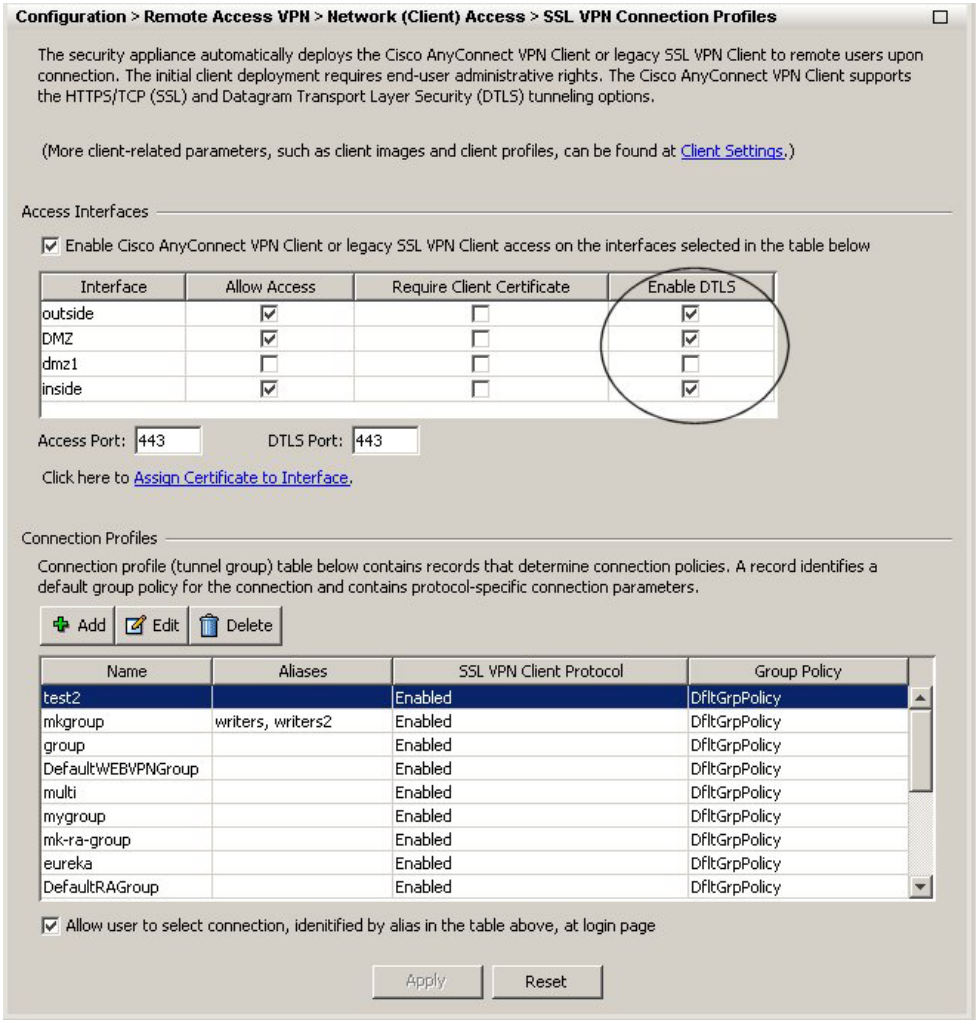
Datagram Transport Layer Security (DTLS) allows the AnyConnect client establishing an SSL VPN connection to use two simultaneous tunnels—an SSL tunnel and a DTLS tunnel. Using DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications 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 5-1).

Figure 5-1 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.

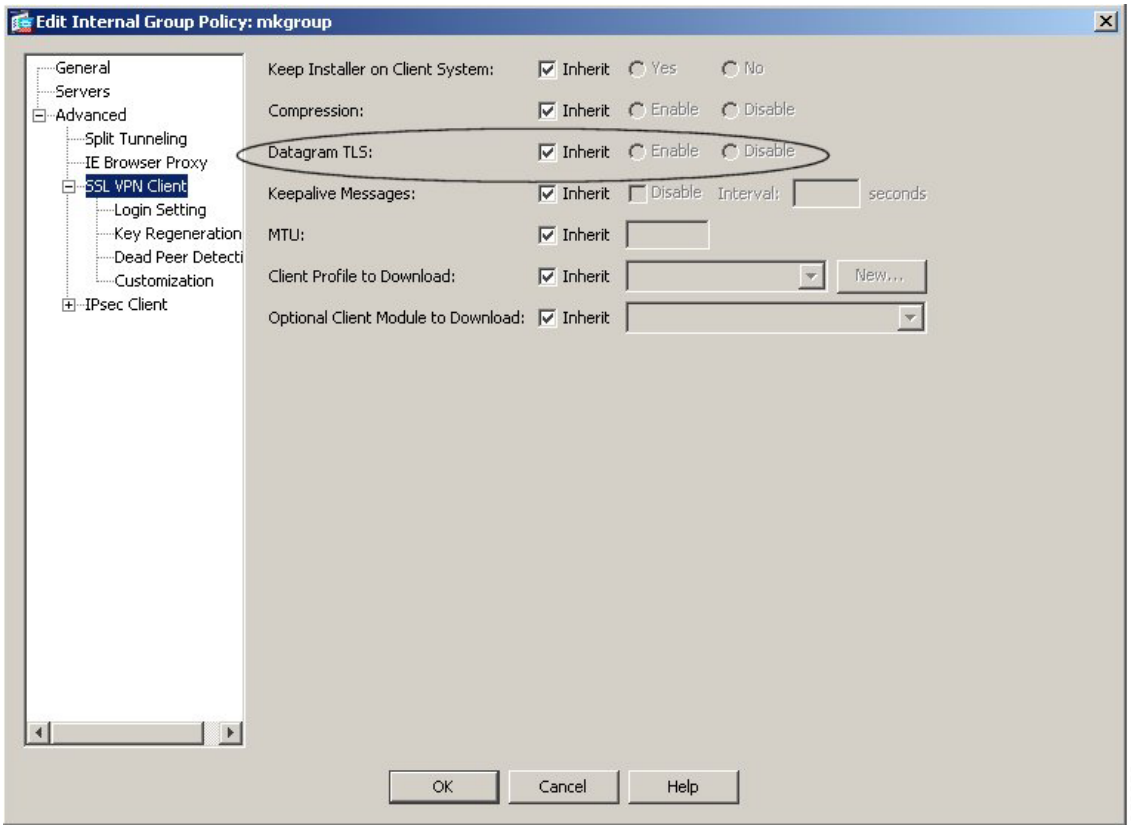
Enabling DTLS allows the AnyConnect client establishing an AnyConnect VPN connection to use two simultaneous tunnels—an SSL tunnel and a DTLS tunnel. Using DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive 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 5-2 shows an example of configuring the DTLS setting for an internal group policy.

Figure 5-2 Enabling or Disabling DTLS

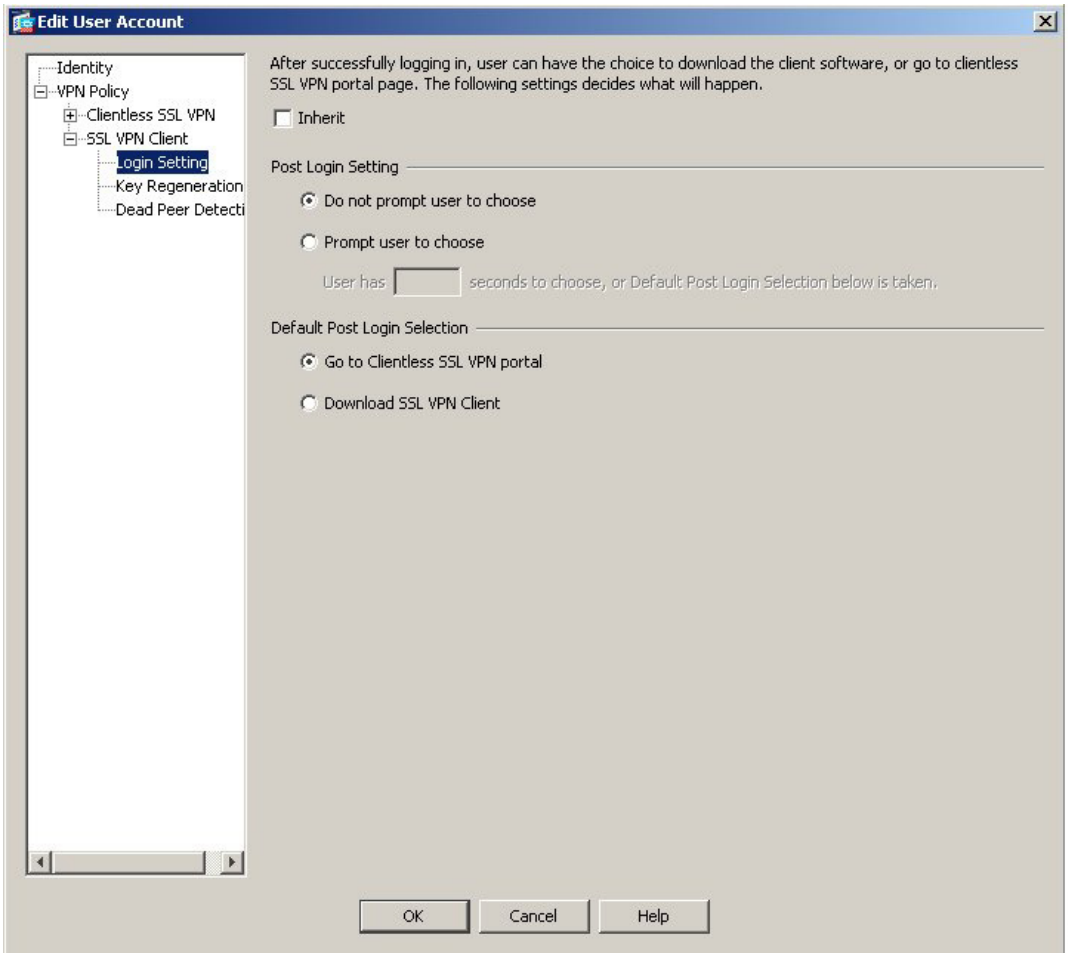


Note When using the AnyConnect client with DTLS on security appliance, Dead Peer Detection must be enabled in the group policy on the security appliance to allow the AnyConnect client to fall back to TLS, if necessary. Fallback to TLS occurs if the AnyConnect client cannot send data over the UPD/DTLS 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 5-3).

Figure 5-3 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.

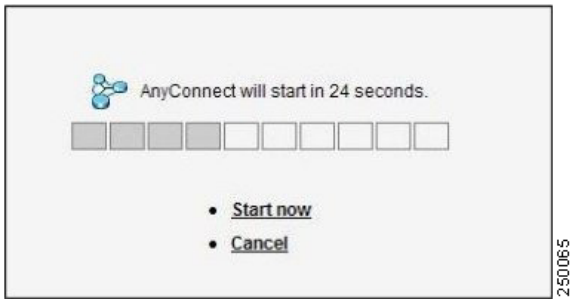
When you enable the prompting option, another field becomes available, asking you to specify the number of seconds the user has to choose before the Default Post Login selection takes effect.

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 5-4 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 5-4 Prompt Displayed to Remote Users for SSL VPN Client Download



Enabling IPv6 VPN Access

The AnyConnect client allows access to IPv6 resources over a public IPv4 connection (Windows XP SP2, Windows Vista, Mac OSX, and Linux only). You must use the command-line interface to configure IPv6; ASDM does not support IPv6.

For more information about enabling IPv6, see Chapter 6, "Configuring AnyConnect Features Using CLI."

Enabling Modules for Additional AnyConnect Features

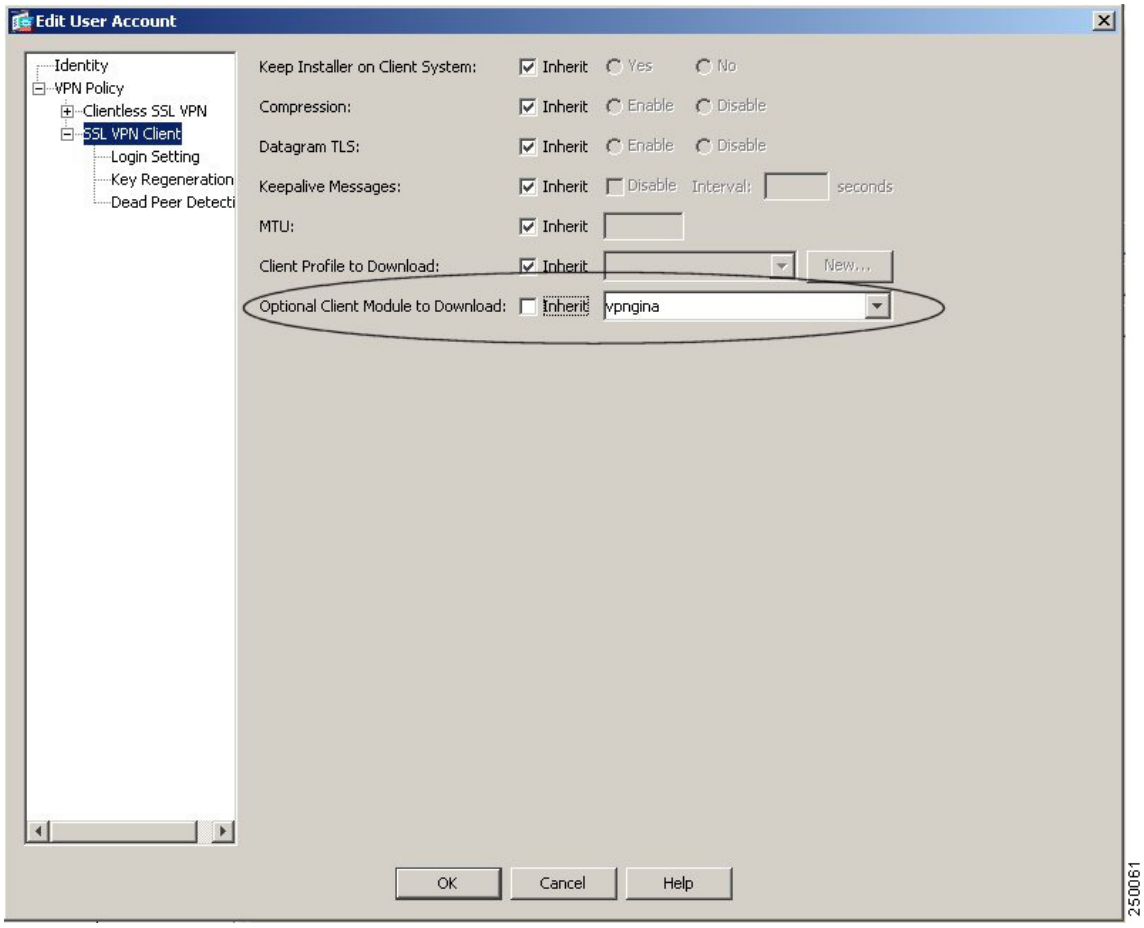
As new features are released for the AnyConnect client, you must update the AnyConnect clients of your remote users for them to use the new features. To minimize download time, the AnyConnect client requests downloads (from the security appliance) only of modules that it needs for each feature that it 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, **sbl** for the Start Before Logon feature, in the Optional Client Module to Download field. Separate multiple strings with commas. Figure 5-5 shows an example.

Figure 5-5 Optional Client Module to Download



In the case of Start Before Logon, you must also enable the feature in the XML profile.

For a list of values to enter for each AnyConnect client feature, see the Release Notes for the Cisco AnyConnect VPN Client.

Configuring, Enabling, and Using Other AnyConnect Features

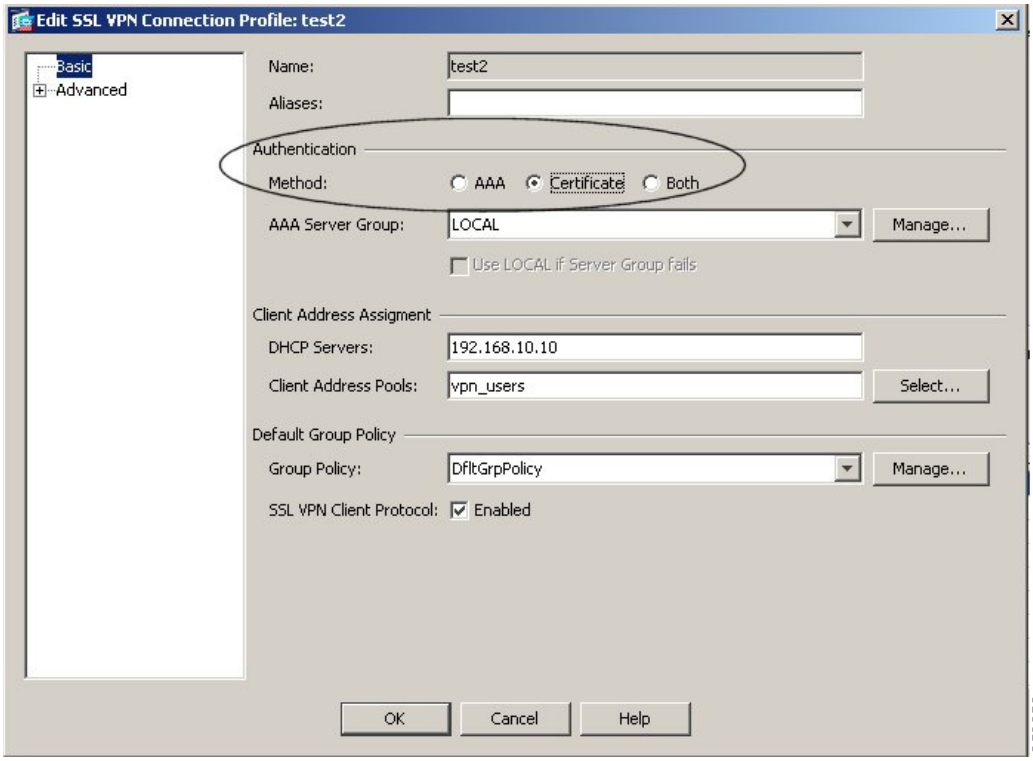
The following sections describe how to configure other AnyConnect features. Some features, such as Secure Desktop and dynamic access policies, do not require that you specifically configure the AnyConnect client to interact with that feature. Rather, all configuration for those features occurs on the 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 digital certificate and are not required to provide a user ID and password.

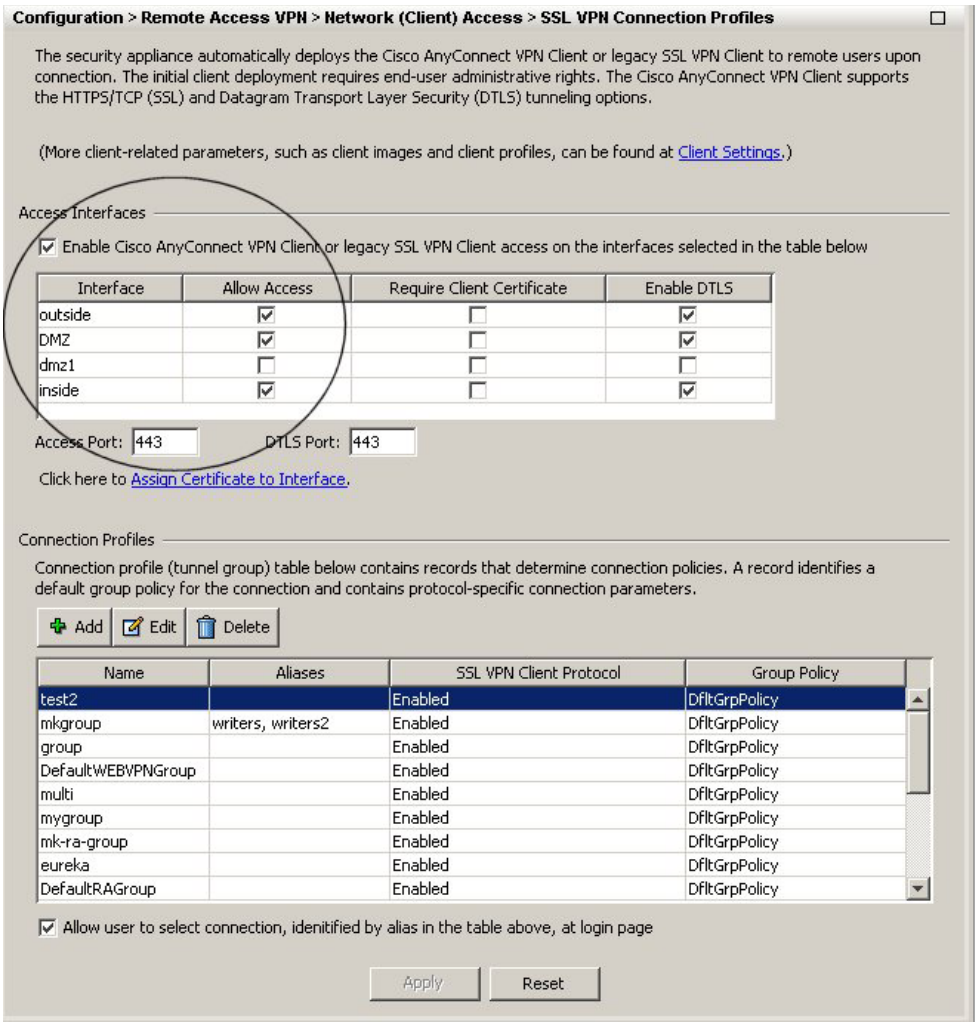
To configure certificate-only authentication using ASDM, select Configuration > Remote Access > Network (Client) Access > SSL VPN Connection Profiles, and in the Connection Profiles area, select Add or Edit. This displays the Add or Edit SSL VPN Connect Profile dialog box with the Basic option selected.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

Figure 5-6 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 5-7) appears.

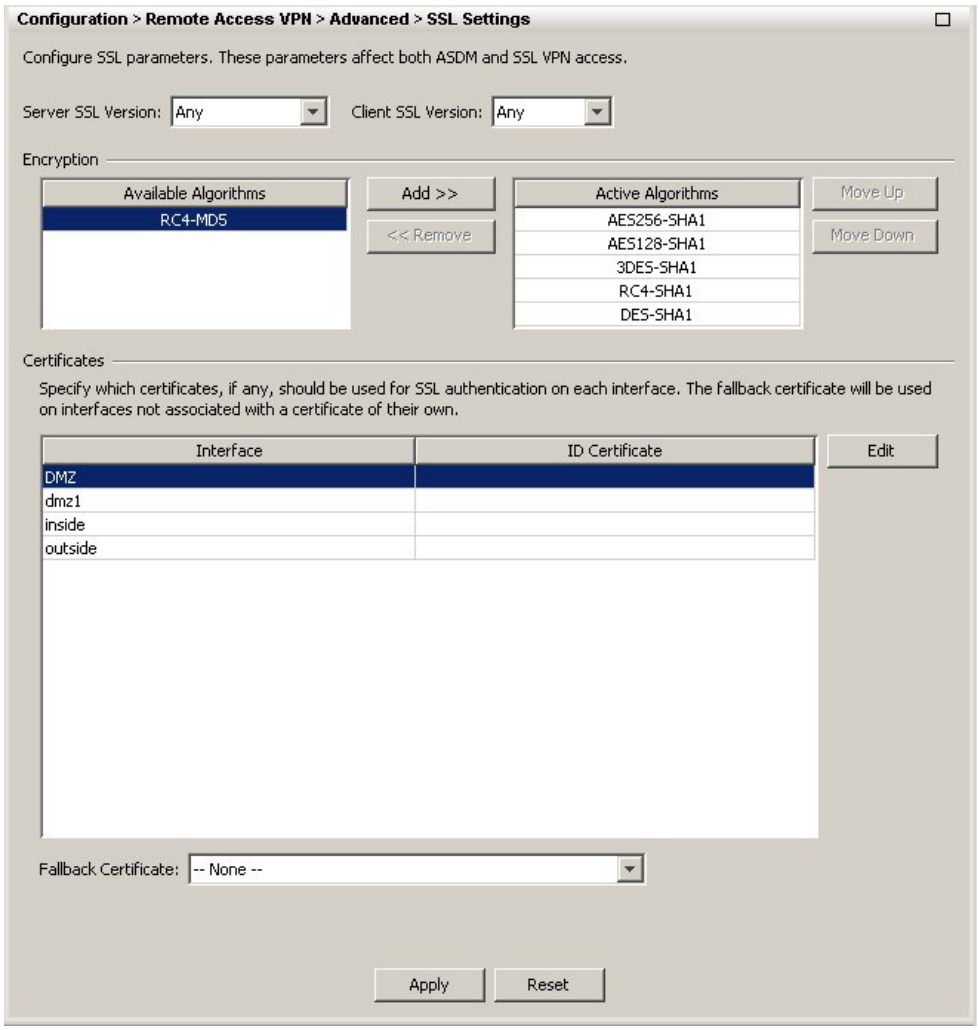
Figure 5-7 SSL VPN Connection Profiles Dialog Box



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 5-8).

Figure 5-8 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.

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

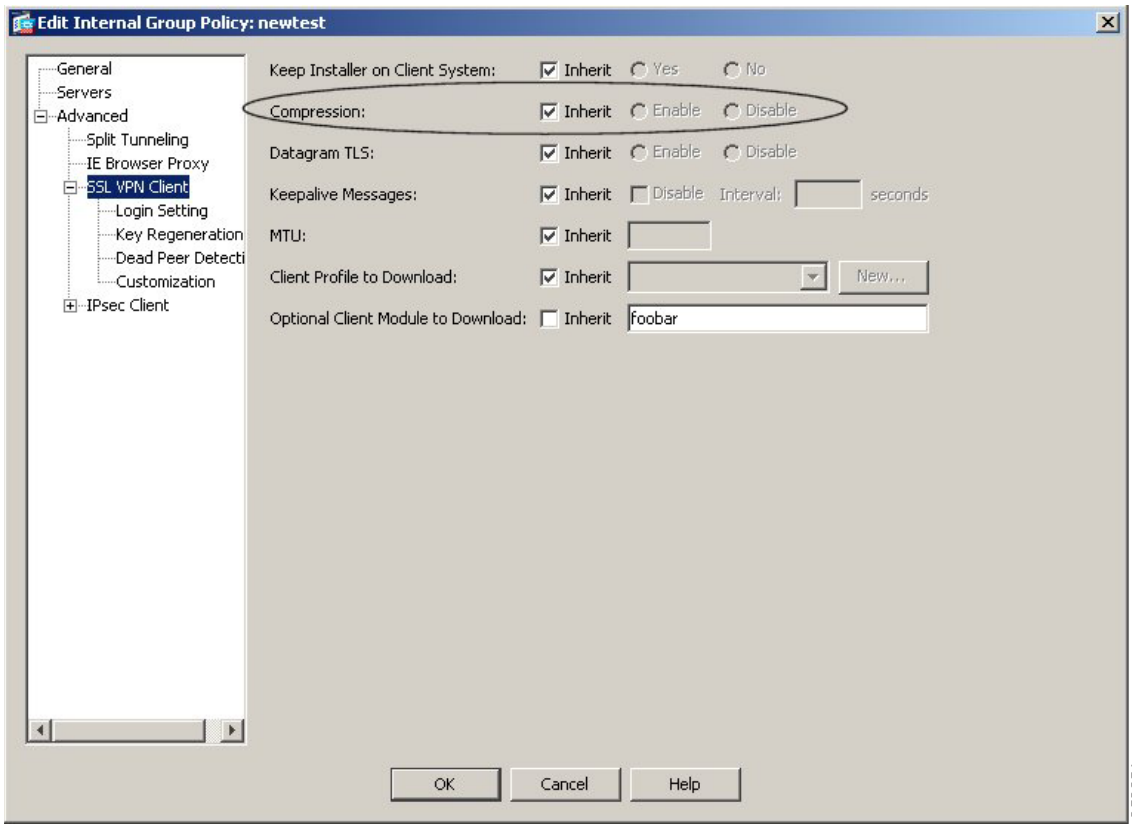
You can also configure compression for specific groups or users using ASDM with the **svc compression** command in group-policy and username webvpn modes. The global setting overrides the group-policy and username settings.

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 5-9 shows an example of configuring the compression setting for an internal group policy.

Figure 5-9 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.

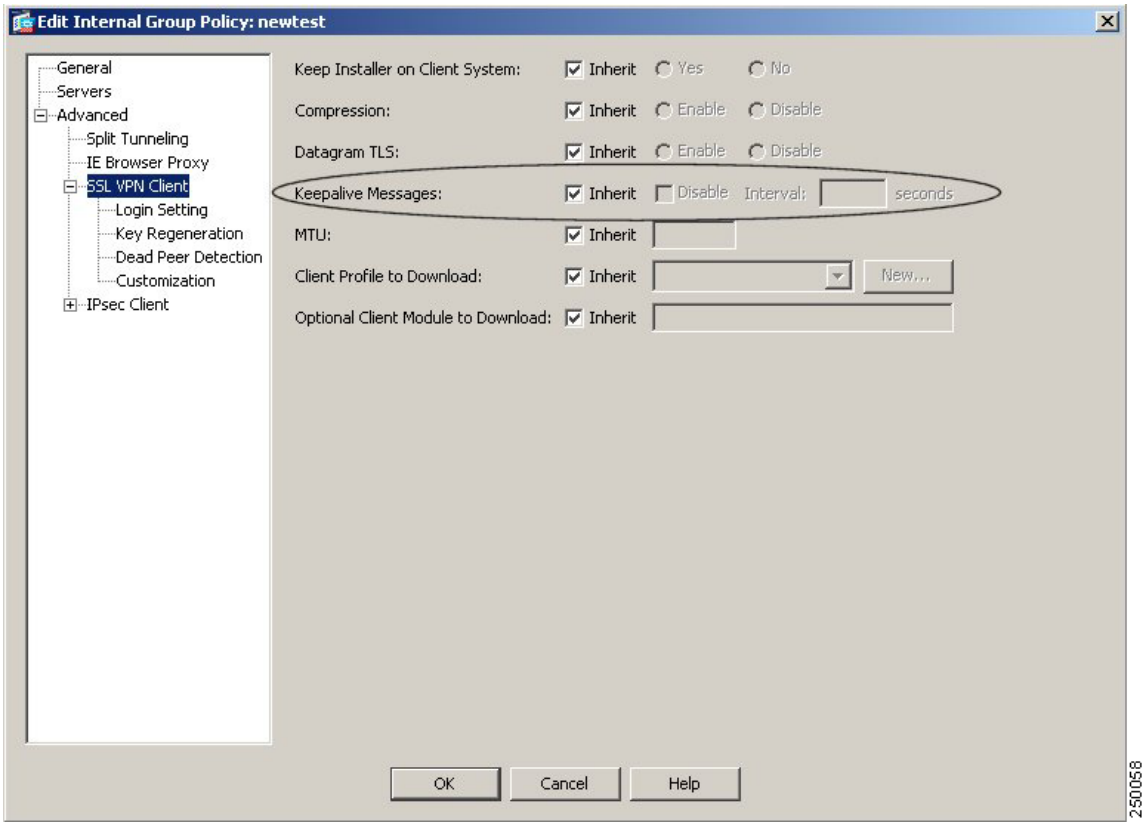
To set the frequency of keepalive messages, use the Keepalive Messages setting in either Group Policy or Username. The paths to this setting are:

- 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 5-10 shows an example of configuring the keepalive messages setting for an internal group policy.

Figure 5-10 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.

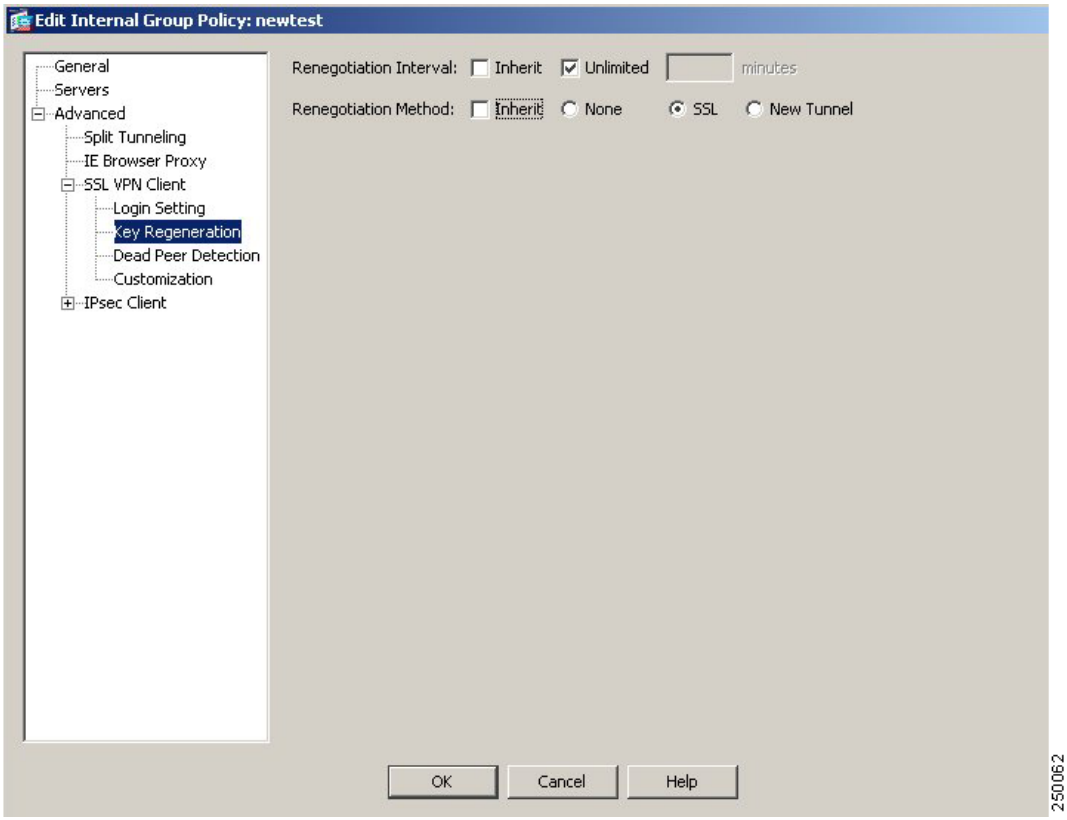
To enable Rekey, use the Key Regeneration dialog box in either Group Policy or Username. The paths to this setting are:

- 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 5-11 shows an example of configuring the Rekey setting for an internal group policy.

Figure 5-11 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 (CSCsh93610).

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.

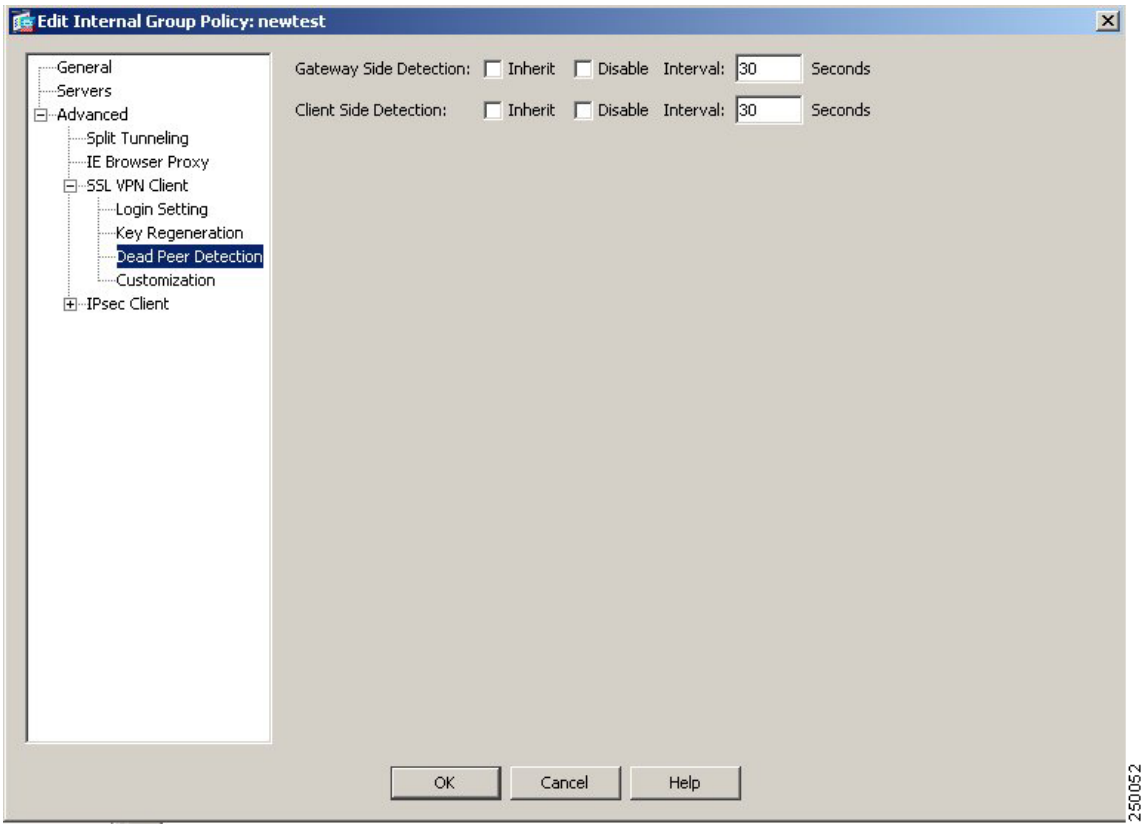
Note When using the AnyConnect client with DTLS on security appliance, Dead Peer Detection must be enabled in the group policy on the security appliance to allow the AnyConnect client to fall back to TLS, if necessary. Fallback to TLS occurs if the AnyConnect client cannot send data over the UPD/DTLS 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 5-12 shows an example of configuring the Dead Peer Detection setting for an internal group policy.

Figure 5-12 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.*

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 3.2)*.