CHAPTER 3

Installing the AnyConnect Client and Configuring the Security Appliance with ASDM

Installing the client on the security appliance consists of copying a client image to the security appliance and identifying the file to the security appliance as a client image. With multiple clients, you must also assign the order in which the security appliance loads the clients to the remote PC.

Note The AnyConnect client configuration uses the same parameters as the SSL VPN Client. Many of the file names, panel names, and ASDM navigation elements, as well as most of the CLI commands include the prefix **svc**, indicating this similarity.

Perform the following steps to install the client:

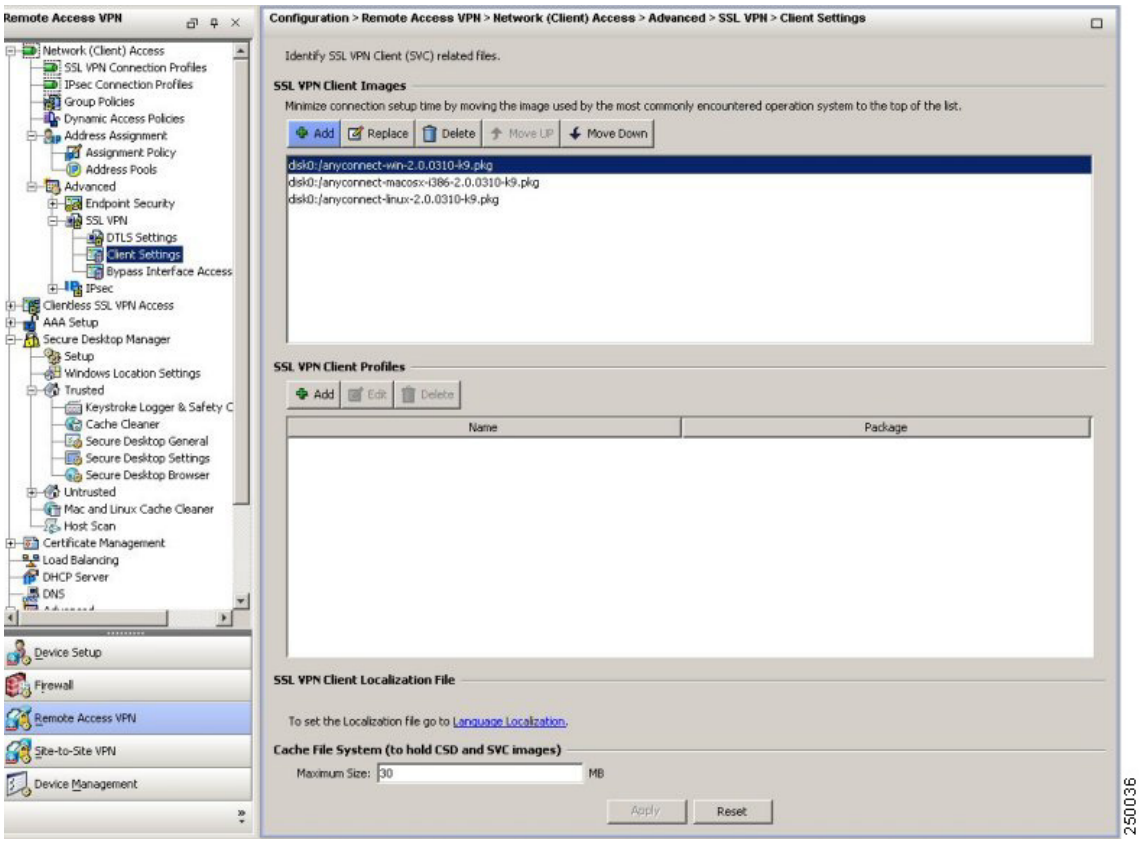
Step 1 Load the AnyConnect client images to the security appliance. On the ASDM toolbar, click **Configuration**. The navigation pane displays features to configure.

Step 2 In the navigation pane, click **Remote Access VPN**. The navigation pane displays VPN features.

Step 3 Choose **Network (Client) Access > Advanced > SSL VPN > Client Settings**. The SSL VPN Client Settings panel displays. (Figure 3-1).

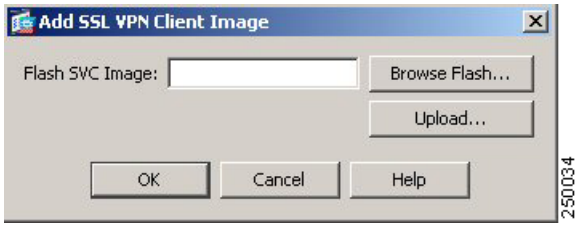
This panel lists any AnyConnect client files that have been identified as AnyConnect client images. The order in which they appear in the table reflects the order in which they download to the remote computer.

Figure 3-1 SSL VPN Client Panel



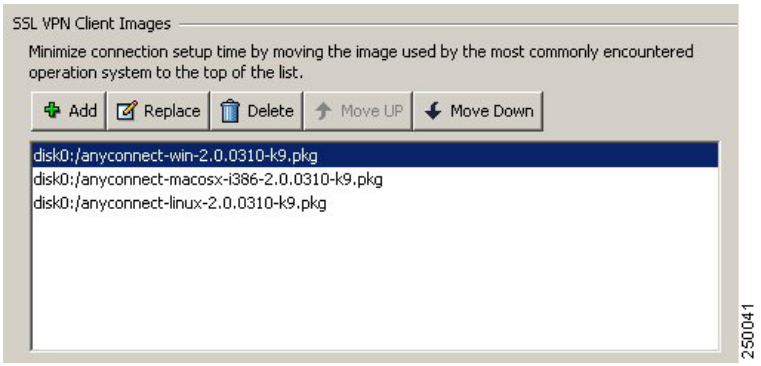
To add an AnyConnect client image, Click **Add** in the SSL VPN Client Images area. The Add SSL VPN Client Image dialog appears (Figure 3-2).

Figure 3-2 Add SSL VPN Client Image Dialog



If you already have an image located in the flash memory of the security appliance, you can enter the name of the image in the Flash SVC Image field, and click **OK**. The SSL VPN Client Settings panel now shows the AnyConnect client images you identified (Figure 3-3).

Figure 3-3 SSL VPN Client Panel with AnyConnect Client Images



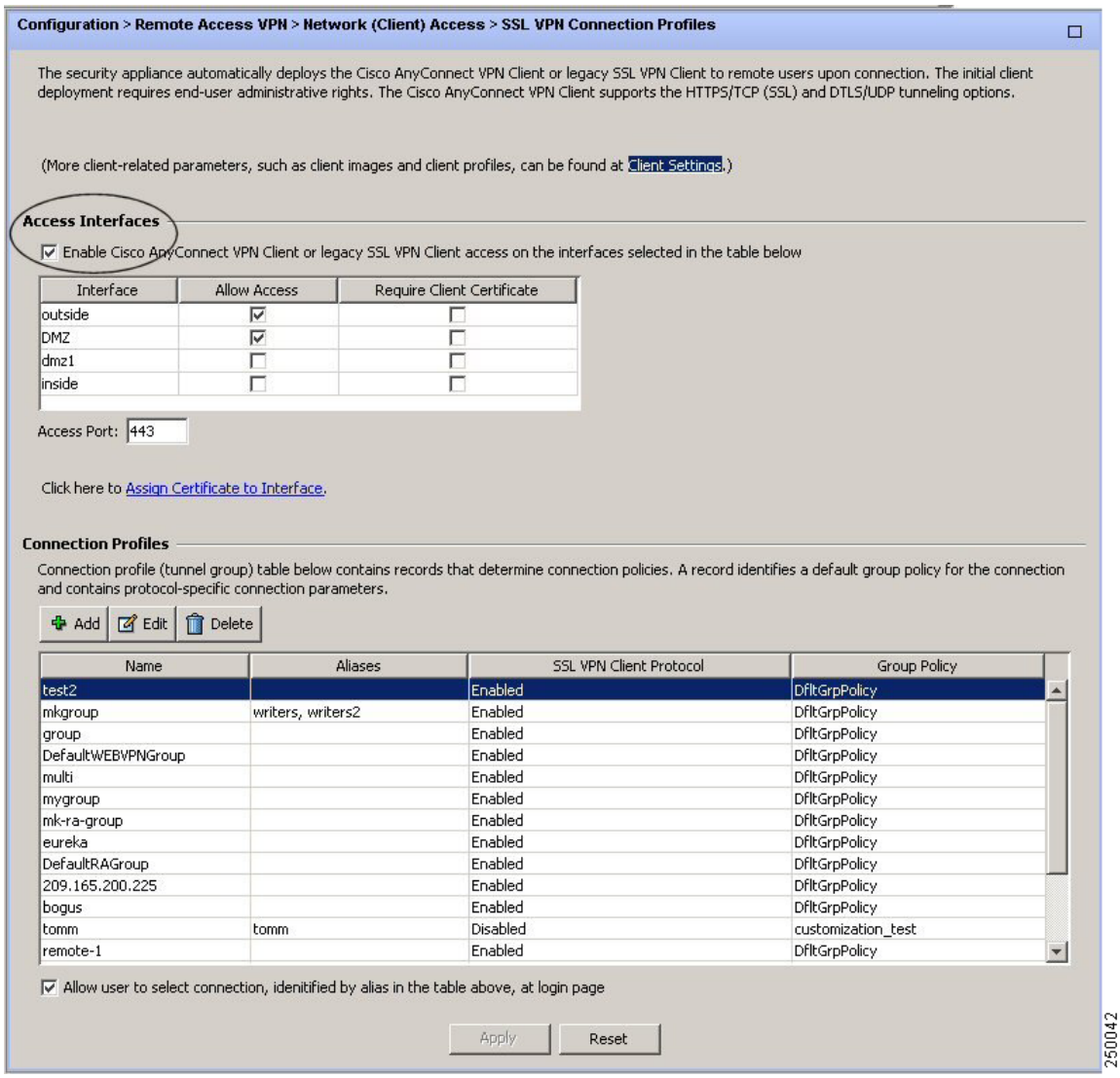
Note The security appliance downloads portions of each client in the order you specify until it matches the operating system of the remote PC. Therefore, assign the topmost position to the image used by the most commonly-encountered operating system.

Step 4 Click on an image name, and use the **Move Up** or **Move Down** button to change the position of the image within the list.

This establishes the order in which the security appliance loads them to the remote computer. The security appliance loads the AnyConnect client image at the top of the list of images first. Therefore, you should move the image used by the most commonly-encountered operating system to the top of the list.

Step 5 Enable the security appliance to download the AnyConnect client to remote users. Go to **Network (Client) Access > SSL VPN Connection Profiles**. The SSL VPN Connection Profiles panel appears (Figure 3-4). Check Enable Cisco AnyConnect VPN Client or legacy SSL VPN client access on the interfaces selected in the table below.

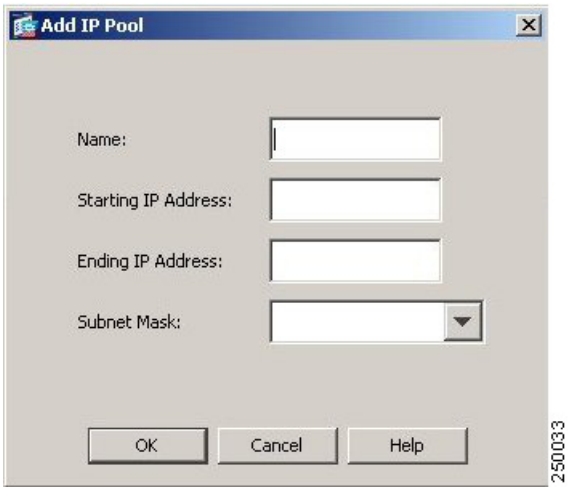
Figure 3-4 Enable SSL VPN Client Check Box



Step 6 Configure a method of address assignment. You can use DHCP, and/or user-assigned addressing. You can also create a local IP address pool and assign the pool to a tunnel group.

To create an IP address pool, choose **Network (Client) Access > Address Management > Address Pools**. Click **Add**. The Add IP Pool dialog appears (Figure 3-5).

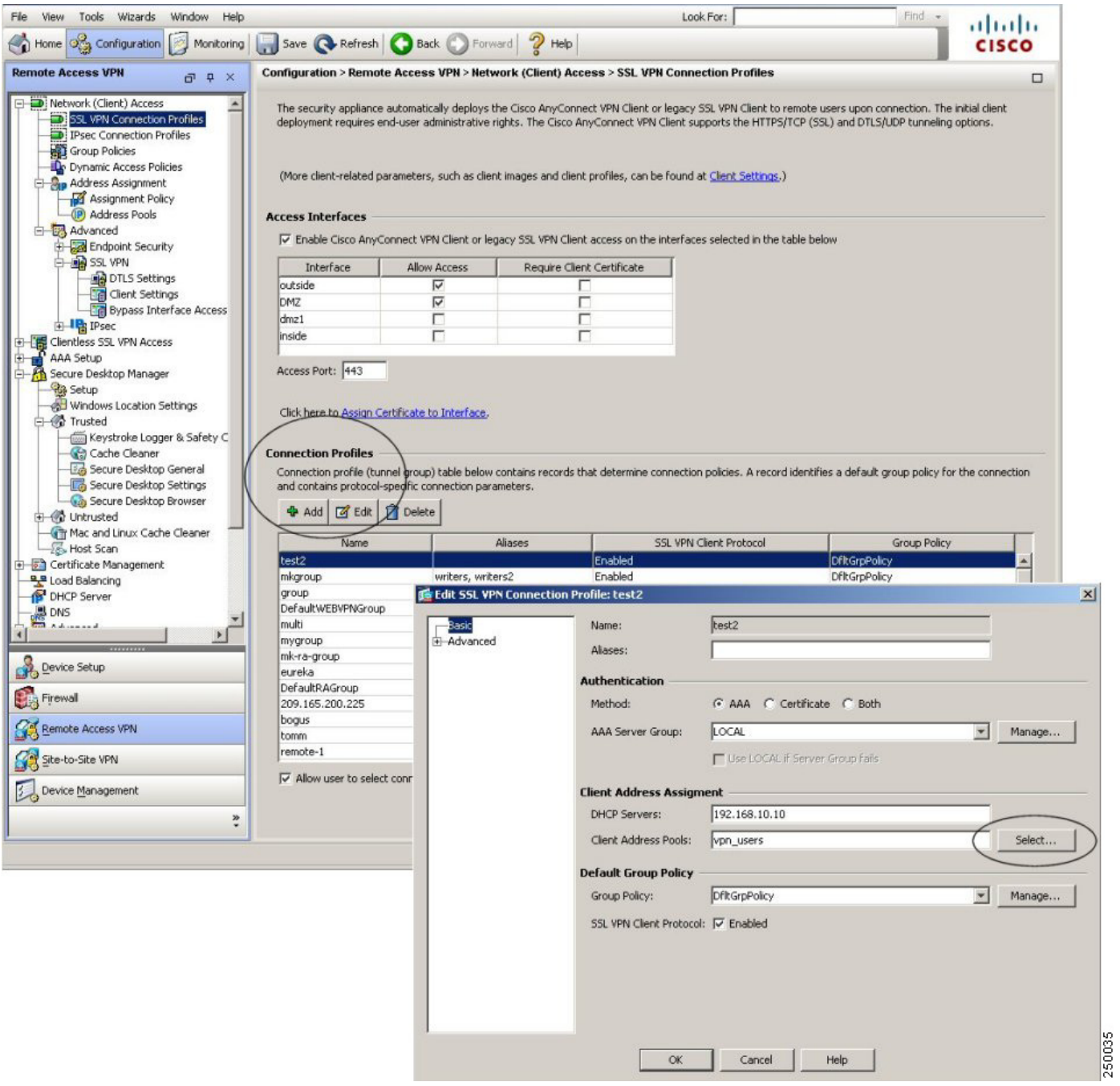
Figure 3-5 Add IP Pool Dialog



Enter the name of the new IP address pool. Enter the starting and ending IP addresses, and enter the subnet mask and click **OK**.

Step 7 Assign the IP address pool to a Connection (tunnel group). To do this, choose **Network (Client) Access > SSL VPN Connection Profiles**. The SSL VPN Connection Profiles panel appears (Figure 3-6):

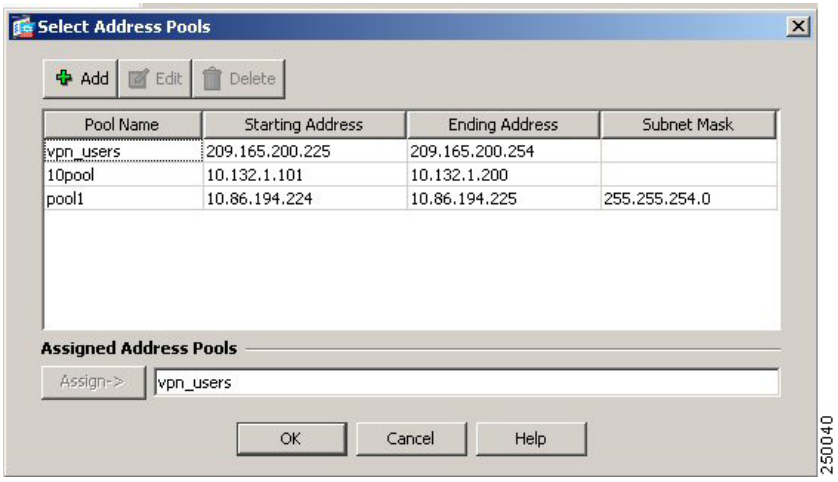
Figure 3-6 Client Address Pool Assignment



To edit an existing connection profile, highlight a connection in the table, and click **Edit.** The Edit SSL VPN Connection > Basic dialog box appears. To add a new connection profile, click Add. The Add SSL VPN Connection > Basic dialog box appears, which is identical to the Edit dialog box, except that you must supply a name for the connection profile. Then proceed as follows.

Click **Select** in the Client Address Assignment area. The Select Address Pool dialog box appears (Figure 3-7), containing available address pools. Select a pool The pool you select appears in the Assign field in the Assigned Address pools area. Click **OK**.

Figure 3-7 Select Address Pool Dialog

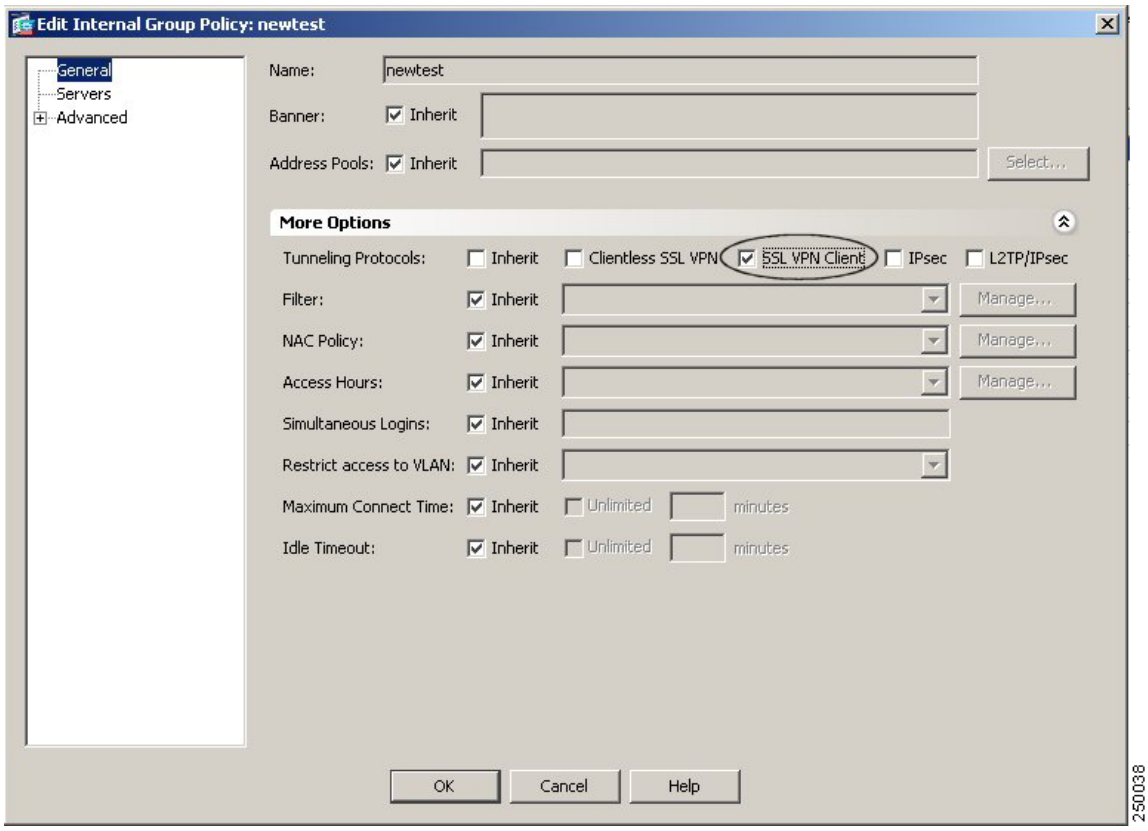


Step 8 Identify SSL VPN as a permitted VPN tunneling protocol for the group or user.

Choose **Network (Client) Access > Group Policies** from the navigation pane. Highlight the group policy in the Group Policy table, and click **Edit**.

The Edit Internal Group Policy dialog appears (Figure 3-8):

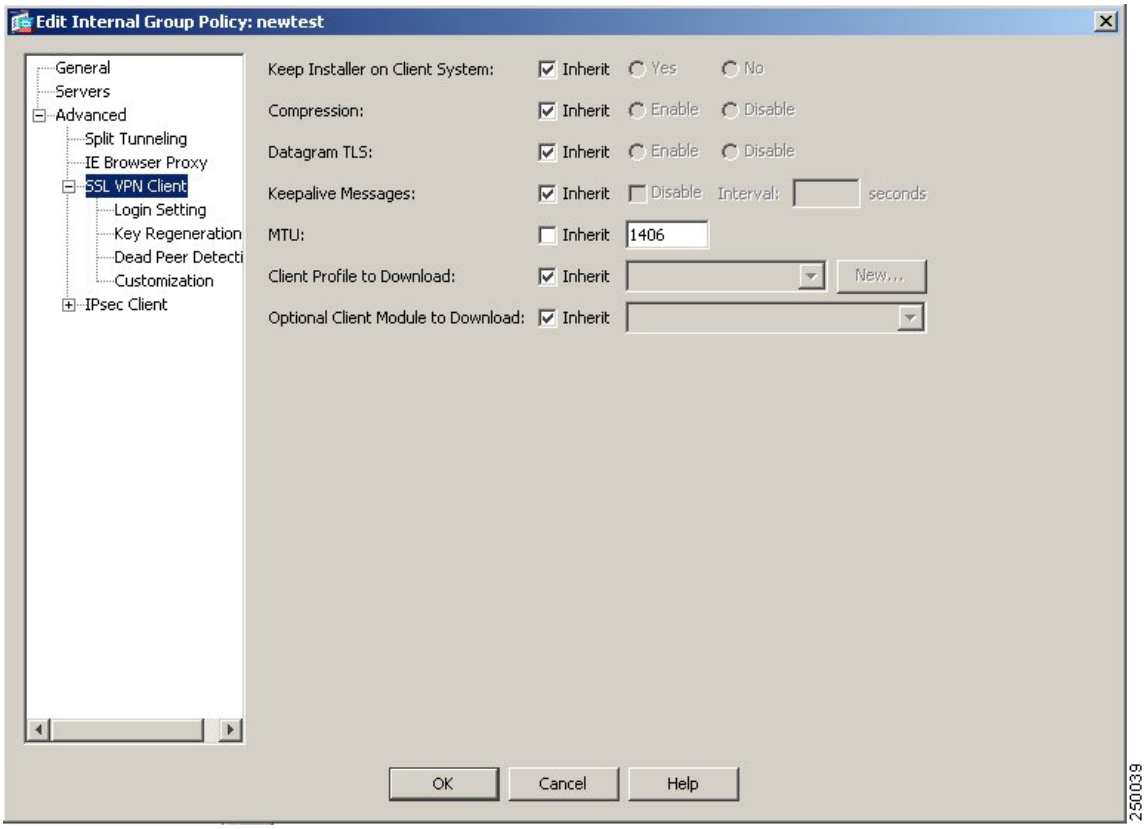
Figure 3-8 Edit Internal Group Policy, General Tab



Check the **SSL VPN Client** check box to include SSL VPN as a tunneling protocol.

Step 9 Configure SSL VPN attributes for a user or group. To display SSL VPN features for groups, In the navigation pane of the Internal Group Policy dialog, choose **Advanced > SSL VPN Client**. The SSL VPN Client features display Figure 3-9.

Figure 3-9 SSL VPN Client Features



Configure the following features on the SSL VPN Client tab:

- **Keep Installer on Client System**—Enable to allow permanent client installation on the remote computer. Enabling disables the automatic uninstalling feature of the client. The client remains installed on the remote computer for subsequent connections, reducing the connection time for the remote user.
- **Compression**—Compression increases the communications performance on low-bandwidth links between the security appliance and the client by reducing the size of the packets being transferred. On broadband connections, compression might degrade performance.
- **Datagram TLS**—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 SSL connections and improves the performance of real-time applications that are sensitive to packet delays.

Note Compression and DTLS are mutually exclusive. If you enable both, DTLS is inactive for the client connection.

- **Keepalive Messages**—Enter an 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.
- **MTU**—Adjust the Maximum Transmission Unit (MTU) in bytes, from 256 to 1406 bytes. This setting affects only the AnyConnect client connections established in SSL, with or without DTLS. By default, the MTU size adjusts automatically based on the MTU of the interface that the connection uses, minus the IP/UDP/DTLS overhead.
- **Client Profile to Download**—Specify a file on flash as a client profile. A profile is a group of configuration parameters that the AnyConnect Client uses to configure the connection entries that appear in the client user interface, including the names and addresses of host computers.
- **Optional Client Module to Download**—Specify any modules that the AnyConnect client needs to download to enable more features, such as Start Before Logon (SBL). To minimize download time, the AnyConnect Client requests downloads (from the security appliance) only of core modules that it needs for each feature that it supports.

The attributes you configure on the Group Policies > Advanced > SSL VPN Client dialog box set the profile for the AnyConnect Client.