



CHAPTER 4

Installing the AnyConnect Client on a Security Appliance Using CLI

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



Note

The AnyConnect client configuration uses the same parameters as the SSL VPN Client. Most of the CLI commands and many of the file names include the prefix **svc**, indicating this similarity.

Perform the following steps to install the client:

- Step 1** Copy the client image package to the security appliance using the **copy** command from privileged EXEC mode, or using another method. This example copies the images from a tftp server using the **copy tftp** command:

```
hostname# copy tftp flash
Address or name of remote host []? 209.165.200.226
Source filename []? anyconnect-win-2.0.0.0343.pkg
Destination filename []? anyconnect-win-2.0.0.0343.pkg
Accessing
tftp://209.165.200.226/anyconnect-win-2.0.0.0343.pkg...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file
disk0:/cdisk71...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
319662 bytes copied in 3.695 secs (86511 bytes/sec)
```

- Step 2** Identify a file on flash as an SSL VPN client package file using the **svc image** command from webvpn configuration mode:

svc image filename order

The security appliance expands the file in cache memory for downloading to remote PCs. If you have multiple clients, assign an order to the client images with the order argument.

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 lowest number to the image used by the most commonly-encountered operating system. For example:

```
hostname(config-webvpn)# svc image anyconnect-win-2.0.0343-k9.pkg 1
hostname(config-webvpn)# svc image anyconnect-macosx-1386-2.0.0343-k9.pkg 2
hostname(config-webvpn)# svc image anyconnect-linux-2.0.0343-k9.pkg 3
```

**Note**

The security appliance expands SSL VPN client and the Cisco Secure Desktop images in cache memory. If you receive the error message *ERROR: Unable to load SVC image - increase disk space via the 'cache-fs' command*, use the **cache-fs limit** command to adjust the size of cache memory:

Step 3 Check the status of the clients using the **show webvpn svc** command:

```
hostname(config-webvpn)# show webvpn svc
1. disk0:/anyconnect-win-2.0.0343-k9.pkg 1
   CISCO STC win2k+
   2,0,0343
   Tue 03/27/2007 4:16:21.09

2. disk0:/anyconnect-macosx-i386-2.0.0343-k9.pkg 2
   CISCO STC Darwin_i386
   2,0,0
   Tue Mar 27 05:09:16 MDT 2007

3. disk0:/anyconnect-linux-2.0.0343-k9.pkg 3
   CISCO STC Linux
   2,0,0
   Tue Mar 27 04:06:53 MST 2007

3 SSL VPN Client(s) installed
```

Enabling AnyConnect Client SSL VPN Connections Using CLI

After installing the client, enable the security appliance to allow AnyConnect VPN client SSL VPN connections by performing the following steps:

Step 1 Enable WebVPN on an interface using the **enable** command from webvpn mode:

enable interface

For example:

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
```

You must enable WebVPN on the interface before enabling DTLS.

Step 2 Enable SSL VPN connections globally, using the **svc enable** command from webvpn configuration mode.

For example:

```
hostname(config-webvpn)# svc enable
```

Step 3 Enable DTLS on an interface, using the **dtls enable** command in webvpn mode. For example:

```
hostname(config-webvpn)# dtls enable outside
```

To enable DTLS globally for a specific port, use the **dtls port** command in webvpn mode. The following example enters webvpn configuration mode and specifies port 444 for DTLS:

```
hostname(config)# webvp4
hostname(config-webvpn)# dtls port 445
```

Step 4 Configure a method of address assignment. You can use DHCP, and/or user-assigned addressing. You can also create a local IP address pool using the **ip local pool** command from global configuration mode:

ip local pool *poolname startaddr-endaddr mask mask*

The following example creates the local IP address pool *vpn_users*:

```
hostname(config)# ip local pool vpn_users 209.165.200.225-209.165.200.254
mask 255.255.255.224
```

- Step 5** Assign IP addresses to a tunnel group. One method you can use to do this is to assign a local IP address pool with the **address-pool** command from general-attributes mode:

address-pool *poolname*

To do this, first enter the **tunnel-group name general-attributes** command to enter general-attributes mode. Then specify the local IP address pool using the **address-pool** command.

In the following example, the user configures the existing tunnel group *telecommuters* to use the address pool *vpn_users* created in step 3:

```
hostname(config)# tunnel-group telecommuters general-attributes
hostname(config-tunnel-general)# address-pool vpn_users
```

- Step 6** Assign a default group policy to the tunnel group with the **default-group-policy** command from tunnel group general attributes mode:

default-group-policy *name*

In the following example, the user assigns the group policy *sales* to the tunnel group *telecommuters*:

```
hostname(config-tunnel-general)# default-group-policy sales
```

- Step 7** Create and enable a group alias that displays in the group list on the WebVPN Login page using the **group-alias** command from tunnel group webvpn attributes mode:

group-alias *name enable*

First exit to global configuration mode, and then enter the **tunnel-group name webvpn-attributes** command to enter tunnel group webvpn attributes mode.

In the following example, the user enters webvpn attributes configuration mode for the tunnel group *telecommuters*, and creates the group alias *sales_department*:

```
hostname(config)# tunnel-group telecommuters webvpn-attributes
hostname(config-tunnel-webvpn)# group-alias sales_department enable
```

- Step 8** Enable the display of the tunnel-group list on the WebVPN Login page from webvpn mode:

tunnel-group-list *enable*

First exit to global configuration mode, and then enter webvpn mode.

In the following example, the user enters webvpn mode, and then enables the tunnel group list:

```
hostname(config)# webvpn
hostname(config-webvpn)# tunnel-group-list enable
```

- Step 9** Specify SSL as a permitted VPN tunneling protocol for the group or user with the **vpn-tunnel-protocol svc** command in group-policy mode or username mode:

vpn-tunnel-protocol *svc*

You can also specify other protocols to permit by adding the names of those protocols to this command. For more information about the **vpn-tunnel-protocol** command, see the command description in *Cisco Security Appliance Command Reference*.

To specify SSL as a permitted tunneling protocol, first exit to global configuration mode, enter the **group-policy name attributes** command to enter group-policy mode, or the **username name attributes** command to enter username mode, and then enter the **webvpn** command to enter webvpn mode and change the WebVPN settings for the group or user.

The following example identifies SSL as the only permitted tunneling protocol for the group-policy *sales*:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# vpn-tunnel-protocol svc
```

For more information about assigning users to group policies, see “Configuring Tunnel Groups, Group Policies, and Users” in *Cisco Security Appliance Command Line Configuration Guide*.

Disabling Permanent Client Installation

Disabling permanent AnyConnect client installation enables the automatic uninstalling feature of the client. The client on the remote computer uninstalls at the end of every session.

To disable permanent AnyConnect client installation for a specific group or user, use the **svc keep-installer** command from group-policy or username webvpn modes:

svc keep-installer none

The default is that permanent installation of the client is enabled. The client on the remote computer remains installed on the remote computer at the end of every session, reducing the connection time for subsequent connections. The following example configures the existing group-policy *sales* to *not* keep the client installed on the remote computer when the session terminates:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-policy)# svc keep-installer none
```