CHAPTER 38

Configuring SSL VPN Client

The SSL VPN Client (SVC) is a VPN tunneling technology that gives remote users the benefits of an IPSec VPN client without the need for network administrators to install and configure IPSec VPN clients on remote computers. The SVC uses the SSL encryption that is already present on the remote computer as well as the WebVPN login and authentication of the security appliance.

To establish an SVC session, the remote user enters the IP address of a WebVPN interface of the security appliance in the browser, and the browser connects to that interface and displays the WebVPN login screen. If the user satisfies the login and authentication, and the security appliance identifies the user as *requiring* the SVC, the security appliance downloads the SVC to the remote computer. If the security appliance identifies the user as having the *option* to use the SVC, the security appliance downloads the SVC to the remote computer while presenting a link on the user screen to skip the SVC installation.

After downloading, the SVC installs and configures itself, and then the SVC either remains or uninstalls itself (depending on the configuration) from the remote computer when the connection terminates.

This section covers the following topics:

Installing SVC

This section presents the platform requirements and the procedure for installing SVC.

Platform Requirements

The SVC requires Windows 2000 or Windows XP on the remote computer.

Installing the SVC Software

Installing SVC consists of copying the SVC images to the security appliance and assigning an order to the images. Perform the following steps to install SVC:

Step 1 Copy the SVC images to the security appliance using the **copy** command from privileged EXEC mode, or using another method. In this example, the images are copied from a tftp server using the **copy tftp** comand:

```
hostname# copy tftp flash
Address or name of remote host []? 209.165.200.226
Source filename []? sslclient-win-1.0.2.127.pkg
Destination filename []? sslclient-win-1.0.2.127.pkg
Accessing tftp://209.165.200.226/sslclient-win-1.0.2.127.pkg...!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file
disk0:/cdisk71...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
319662 bytes copied in 3.695 secs (86511 bytes/sec)
```

Step 2 Assign an order to the SVC images using the **svc image** command from webvpn mode:

svc image *filename order*

Numbering of the SVC images establishes the order in which the security appliance downloads them to the remote computer. It downloads the SVC image with the lowest number first. Therefore, you should assign the lowest number to the image used by the most commonly-encountered operating system.

In the following example, the output of the **show webvpn svc** command indicates that the windows.pkg image has an order number of 1, and the windows2.pkg image has an order number of 2. When a remote computer attempts to establish an SVC connection, the windows.pkg image downloads first. If the image does not match the operating system, the windows2.pkg image downloads:

```
hostname(config)# webvpn
hostname(config-webvpn)# show webvpn svc
1. disk0:/windows.pkg 1
  CISCO STC win2k+ 1.0.0
  1,0,2,132
  Thu 08/25/2005 21:51:30.43

2. disk0:/windows2.pkg 2
  CISCO STC win2k+ 1.0.0
  1,0,0,164
  Thu 02/17/2005 20:09:22.43

2 SSL VPN Client(s) installed
```

Then the SVC archive images are re-ordered using the **svc image** command, with the windows2.pkg image as the first image downloaded to the remote PC, and the windows.pkg image downloaded second:

```
hostname(config-webvpn)# no svc image
hostname(config-webvpn)# svc image windows2.pkg 1
hostname(config-webvpn)# svc image windows.pkg 2

Reentering the show webvpn svc command shows the new order of the images:

hostname(config-webvpn)# show webvpn svc
1. disk0:/windows2.pkg 1
  CISCO STC win2k+ 1.0.0
  1,0,2,132
  Thu 08/25/2005 21:51:30.43

2. disk0:/windows.pkg 2
  CISCO STC win2k+ 1.0.0
```

```
  1,0,0,164
  Thu 02/17/2005 20:09:22.43

2 SSL VPN Client(s) installed
```

Enabling SVC

After installing SVC, you can enable SVC 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
```

Step 2 From webvpn mode, enter the **svc enable command** to enable the security appliance to download SVC images to remote computers:

svc enable

For example:

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

Step 3 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 webvpn mode:

ip local pool *poolname startaddr-endaddr* **mask** *mask*

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

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

Step 4 Assign IP addresses to a tunnel group. One method you can use to do this is to configure 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 5 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 6 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 7 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 enters webvpn mode, and then enables the tunnel group list:

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

Step 8 Identify WebVPN as a permitted VPN tunneling protocol for the group or user with the **vpn-tunnel-protocol webvpn** command in group-policy mode or username mode:

vpn-tunnel-protocol webvpn

To do this, 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 WebVPN as a 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 webvpn
```

Step 9 Enable or require an SVC for a specific group or user by using the **svc** command from either group-policy webvpn mode or username webvpn mode:

svc {**none** | **enable** | **required**}

The following example sets the SVC to *required* for the existing group-policy *sales*:

```
hostname(config-group-webvpn)# svc required
```

For more information about assigning users to group policies, see Chapter 30, “Configuring Tunnel Groups, Group Policies, and Users”.

Enabling Permanent SVC Installation

Enabling permanent SVC installation disables the automatic uninstalling feature of the SVC. The SVC remains installed on the remote computer for subsequent SVC connections, reducing the SVC connection time for the remote user.

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

svc keep-installer {**installed** | **none**}

no svc keep-installer {**installed** | **none**}

Where:

installed specifies the SVC is permanently installed on the remote computer.

none specifies the SVC is removed from the remote computer after the active SVC connection terminates.

The default is that permanent installation of the SVC is disabled. The SVC on the remote computer uninstalls at the end of every SVC session.

The following example configures the existing group-policy *sales* to keep the SVC installed on the remote computer:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-policy)# svc keep-installer installed
```

Enabling Rekey

When the security appliance and the SVC perform a rekey, they renegotiate the crypto keys and initialization vectors, increasing the security of the connection.

To enable the SVC to perform a rekey on an SVC session for a specific group or user, use the **svc rekey** command from group-policy and username webvpn modes.

svc rekey {**method** {**new-tunnel** | **none** | **ssl**} | **time** *minutes*}

no svc rekey {**method** {**new-tunnel** | **none** | **ssl**} | **time** *minutes*}

Where:

method new-tunnel specifies that the SVC establishes a new tunnel during SVC rekey.

method none disables SVC rekey.

method ssl specifies that SSL renegotiation takes place during SVC rekey.

time *minutes* specifies the number of minutes from the start of the session until the rekey takes place, from 1 to 10080 (1 week).

In the following example, the SVC is configured to renegotiate with SSL during rekey, which takes place 30 minutes after the session begins, for the existing group-policy *sales*:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-policy)# svc rekey method ssl
hostname(config-group-policy)# svc rekey time 30
```

Enabling and Adjusting Dead Peer Detection

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

To enable DPD on the security appliance or SVC for a specific group or user, and to set the frequency with which either the security appliance or SVC performs DPD, use the **svc dpd-interval** command from group-policy or username webvpn mode:

svc dpd-interval {[**gateway** {*seconds* | **none***}]* | [**client** {*seconds* | **none***}]*}

no svc dpd-interval {[**gateway** {*seconds* | **none***}]* | [**client** {*seconds* | **none***}]*}

Where:

gateway seconds enables DPD performed by the security appliance (gateway) and specifies the frequency, from 30 to 3600 seconds, with which the security appliance (gateway) performs DPD.

gateway none disables DPD performed by the security appliance.

client *seconds* enable DPD performed by the SVC (client), and specifies the frequency, from 30 to 3600 seconds, with which the SVC performs DPD.

client none disables DPD performed by the SVC.

To remove the **svc dpd-interval** command from the configuration, use the **no** form of the command:

The following example sets the frequency of DPD performed by the security appliance to 3000 seconds, and the frequency of DPD performed by the SVC set to 1000 seconds for the existing group-policy *sales*:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-policy)# svc dpd-interval gateway 3000
hostname(config-group-policy)# svc dpd-interval client 1000
```

Enabling Keepalive

You can adjust the frequency of keepalive messages to ensure that an SVC 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 SVC 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 **svc keepalive** command from group-policy or username webvpn modes:

svc keepalive {none | *seconds***}**

no svc keepalive {none | *seconds***}**

Where:

none disables SVC keepalive messages.

seconds enables the SVC to send keepalive messages, and specifies the frequency of the messages in the range of 15 to 600 seconds.

The default is keepalive messages are disabled.

Use the **no** form of the command to remove the command from the configuration and cause the value to be inherited:

In the following example, the security appliance is configured to enable the SVC to send keepalive messages with a frequency of 300 seconds (5 minutes), for the existing group-policy *sales*:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc keepalive 300
```

Using SVC Compression

SVC compression increases the communications performance between the security appliance and the SVC by reducing the size of the packets being transferred. By default, compression for all SVC connections is enabled on the security appliance, both at the global level and for specific groups or users.

SVC compression can be set globally using the **compression svc** command from global configuration mode. It can also be set for specific groups or users with the **svc compression** command in group-policy and username webvpn modes. The global setting overrides the group-policy and username settings.

Changing SVC Compression Globally

To change the global SVC 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 SVC connections globally:

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

Changing SVC Compression for Groups and Users

To change compression for a specific group or user, use the **svc compression** command in the group-policy and username webvpn modes:

svc compression {**deflate** | **none**}

no svc compression {**deflate** | **none**}

By default, for groups and users, SVC compression is set to *deflate* (enabled).

To remove the **svc compression** command from the configuration and cause the value to be inherited from the global setting, use the **no** form of the command:

In the following example, SVC compression is disabled for the group-policy sales:

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

Note The **compression svc** command configured from global configuration mode overrides the **svc compression** command configured in group-policy and username webvpn modes.

Viewing SVC Sessions

You can view information about active SVC sessions using the **show vpn-sessiondb** command in privileged EXEC mode:

show vpn-sessiondb svc

The following example shows the output of the **show vpn-sessiondb svc** command:

```
hostname# show vpn-sessiondb svc

Session Type: SSL VPN Client

Username     : lee
Index        : 1                     IP Addr      : 161.44.128.249
Protocol     : SSL VPN Client        Encryption   : 3DES
Hashing      : SHA1                  Auth Mode    : userPassword
TCP Dst Port : 443                   TCP Src Port : 54230
Bytes Tx     : 20178                 Bytes Rx     : 8662
Pkts Tx      : 27                    Pkts Rx      : 19
Client Ver   : Cisco STC 1.1.0.117
Client Type  : Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; Q312461)
Group        : DfltGrpPolicy
Login Time   : 14:32:03 UTC Wed Apr 20 2005
Duration     : 0h:00m:04s
```

```
Filter Name  :
```

Logging Off SVC Sessions

To log off all SVC sessions, use the **vpn-sessiondb logoff svc** command in global configuration mode:

vpn-sessiondb logoff svc

The following example logs off all SVC sessions:

```
hostname# vpn-sessiondb logoff svc
INFO: Number of sessions of type "svc" logged off : 1
```

You can log off individual SVC sessions using either the **name option, or the index option**:

vpn-session-db logoff name *name*

vpn-session-db logoff index *index*

You can find both the username and the index number (established by the order of the SVC images) in the output of the **show vpn-sessiondb svc** command. The following example shows the username *lee* and index number *1*.

```
hostname# show vpn-sessiondb svc

Session Type: SSL VPN Client

Username     : lee
Index        : 1                     IP Addr      : 161.44.128.249
Protocol     : SSL VPN Client        Encryption   : 3DES
Hashing      : SHA1                  Auth Mode    : userPassword
TCP Dst Port : 443                   TCP Src Port : 54230
Bytes Tx     : 20178                 Bytes Rx     : 8662
Pkts Tx      : 27                    Pkts Rx      : 19
Client Ver   : Cisco STC 1.1.0.117
Client Type  : Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; Q312461)
Group        : DfltGrpPolicy
Login Time   : 14:32:03 UTC Wed Apr 20 2005
Duration     : 0h:00m:04s
Filter Name  :
```

The following example terminates the session using the **name** option of the **vpn-session-db logoff command**:

```
hostname# vpn-session-db logoff name lee
INFO: Number of sessions with name "lee" logged off : 1
```

Updating SVCs

You can update the SVC images on the security appliance at any time using the following procedure:

Step 1 Copy the new SVC images to the security appliance using the **copy** command from privileged EXEC mode, or using another method.

Step 2 If the new SVC image files have the same filenames as the files already loaded, reenter the **svc image** command that is in the configuration. If the new filenames are different, uninstall the old files using the **no svc image** command. Then use the **svc image** command to assign an order to the SVC images and cause the security appliance to load the new SVC images.