CHAPTER 6

Configuring AnyConnect Features Using CLI

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

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, SSL VPN connections connect with an SSL VPN tunnel only.

Enabling DTLS Globally for a Specific Port

To enable DTLS globally for a particular port, use the **dtls port** command:

[no] dtls port *port_number*

For example:

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

Enabling DTLS for Specific Groups or Users

To enable DTLS for specific groups or users, use the **svc dtls enable** command in group policy webvpn or username webvpn configuration mode:

[**no**] **svc dtls enable**

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.

The following example enters group policy webvpn configuration mode for the group policy *sales* and enables DTLS:

```
hostname(config)# enable inside
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc dtls enable
```

Prompting Remote Users

You can enable the security appliance to prompt remote AnyConnect VPN client users to download the client with the **svc ask** command from group policy webvpn or username webvpn configuration modes:

[**no**] **svc ask** {**none** | **enable** [**default** {**webvpn** | **svc**} **timeout** *value*]}

svc ask enable prompts the remote user to download the client or go to the WebVPN portal page and waits indefinitely for user response.

svc ask enable default svc immediately downloads the client.

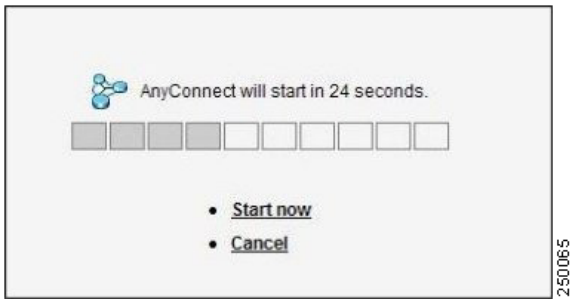
svc ask enable default webvpn immediately goes to the portal page.

svc ask enable default svc timeout *value* prompts the remote user to download the client or go to the WebVPN portal page and waits the duration of *value* before taking the default action—downloading the client.

svc ask enable default webvpn timeout ***value*** prompts the remote user to download the client or go to the WebVPN portal page, and waits the duration of *value* before taking the default action—displaying the WebVPN portal page.

Figure 6-1 shows the prompt displayed to remote users when either **default svc timeout** *value* or **default webvpn timeout** *value* is configured:

Figure 6-1 Prompt Displayed to Remote Users for SSL VPN Client Download



The following example configures the security appliance to prompt the remote user to download the client or go to the WebVPN portal page and to wait 10 seconds for user response before downloading the client:

```
hostname(config-group-webvpn)# svc ask enable default svc timeout 10
```

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.

You enable IPv6 access using the **ipv6 enable** command as part of enabling SSL VPN connections. The following is an example for an IPv6 connection that enables IPv6 on the outside interface:

```
hostname(config)# interface GigabitEthernet0/0
hostname(config-if)# ipv6 enable
```

To enable IPV6 SSL VPN, do the following general actions:

1. Enable IPv6 on the outside interface.
2. Enable IPv6 and an IPv6 address on the inside interface.
3. Configure an IPv6 address local pool for client assigned IP Addresses.
4. Configure an IPv6 Tunnel default gateway.

To implement this procedure, do the following steps:

Step 1 Configure Interfaces:

```
interface GigabitEthernet0/0
     nameif outside
     security-level 0
     ip address 192.168.0.1 255.255.255.0
     ipv6 enable          ; Needed for IPv6.
```

```
    !
interface GigabitEthernet0/1
     nameif inside
     security-level 100
     ip address 10.10.0.1 255.255.0.0
     ipv6 address 2001:DB8::1/32        ; Needed for IPv6.
     ipv6 enable           ; Needed for IPv6.
```

Step 2 Configure an 'ipv6 local pool' (used for AnyConnect Client IPv6 address assignment):

```
ipv6 local pool ipv6pool 2001:DB8:1:1::5/32 100     ; Use your IPv6 prefix here
```

Note You still need to configure an IPv4 address pool when using IPv6 (using the ip local pool command)

Step 3 Add the ipv6 address pool to your Tunnel group policy (or group-policy):

```
tunnel-group YourTunGrp1 general-attributes  ipv6-address-pool ipv6pool
```

Note Again, you must also configure an IPv4 address pool here as well (using the 'address-pool' command).

Step 4 Configure an IPv6 Tunnel Default Gateway:

```
ipv6 route inside ::/0 X:X:X:X::X tunneled
```

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 using the **svc modules** command from group policy webvpn or username webvpn configuration mode:

[**no**] **svc modules** {**none** | **value** *string*}

Separate multiple strings with commas.

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

In the following example, the network administrator enters group-policy attributes mode for the group policy telecommuters, enters webvpn configuration mode for the group policy, and specifies the string vpngina to enable the AnyConnect client feature Start Before Login:

```
hostname(config)# group-policy telecommuters attributes
hostname(config-group-policy)# webvpn
hostame(config-group-webvpn)# svc modules value vpngina
```

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 software package itself.

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 CLI, use the **authentication** command with the keyword **certificate** in tunnel-group webvpn mode. For example:

```
hostname(config)# tunnel-group testgroup webvpn-attributes
asa2(config-tunnel-webvpn)# authentication ?
asa2(config-tunnel-webvpn)# authentication certificate
```

Note You must configure **ssl certificate-authentication interface** <*interface*> **port** <*port*> for this option to take effect.

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, specify only Certificate as the Method.

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.

You can configure compression globally using the **compression svc** command from global configuration mode. You can also configure compression 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 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

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, SSL 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:

The following example disables compression for the group-policy sales:

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

Note For compression to work, both the **compression svc** command (configured from global configuration mode) and the **svc compression** command (configured in group-policy and username webvpn modes) must be enabled. If *either* command is set to **none** or to the **no** form, compression is disabled.

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)*.

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 the client to perform a rekey on an SSL VPN connection for a specific group or user, use the **svc rekey** command from group-policy and username webvpn modes.

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

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

method none disables rekey.

method ssl specifies that SSL renegotiation takes place during rekey.

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

In the following example, the client 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
```

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 (CSC93610).

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 ASA 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 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 client, and specifies the frequency, from 30 to 3600 seconds, with which the client performs DPD.

client none disables DPD performed by the client.

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 30 seconds, and the frequency of DPD performed by the client set to 10 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 30
hostname(config-group-policy)# svc dpd-interval client 10
```

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 **svc keepalive** command from group-policy webvpn or username webvpn configuration mode:

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

none disables client keepalive messages.

seconds enables the client 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 client 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
```