

AnyConnect VPN Client Connections

This section describes how to configure AnyConnect VPN Client Connections and covers the following topics:

- Information About AnyConnect VPN Client Connections, page 11-1
- Licensing Requirements for AnyConnect Connections, page 11-2
- Guidelines and Limitations, page 11-4
- Configuring AnyConnect Connections, page 11-5
- Configuring Advanced AnyConnect SSL Features, page 11-14
- Configuration Examples for Enabling AnyConnect Connections, page 11-20
- Feature History for AnyConnect Connections, page 11-21

Information About AnyConnect VPN Client Connections

The Cisco AnyConnect Secure Mobility Client provides secure SSL and IPsec/IKEv2 connections to the ASA for remote users. Without a previously-installed client, remote users enter the IP address in their browser of an interface configured to accept SSL or IPsec/IKEv2 VPN connections. Unless the ASA is configured to redirect http:// requests to https://, users must enter the URL in the form https://<*address*>.

After entering the URL, the browser connects to that interface and displays the login screen. If the user satisfies the login and authentication, and the ASA identifies the user as requiring the client, it downloads the client that matches the operating system of the remote computer. After downloading, the client installs and configures itself, establishes a secure SSL or IPsec/IKEv2 connection and either remains or uninstalls itself (depending on the configuration) when the connection terminates.

In the case of a previously installed client, when the user authenticates, the ASA examines the revision of the client, and upgrades the client as necessary.

When the client negotiates an SSL VPN connection with the ASA, it connects using Transport Layer Security (TLS), and optionally, Datagram Transport Layer Security (DTLS). 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.

The AnyConnect client can be downloaded from the ASA, or it can be installed manually on the remote PC by the system administrator. For more information about installing the client manually, see the *Cisco AnyConnect VPN Client Administrator Guide*.

The ASA downloads the client based on the group policy or username attributes of the user establishing the connection. You can configure the ASA to automatically download the client, or you can configure it to prompt the remote user about whether to download the client. In the latter case, if the user does not respond, you can configure the ASA to either download the client after a timeout period or present the login page.

Licensing Requirements for AnyConnect Connections

Note This feature is not available on No Payload Encryption models.

Model	License Requirement[1,2]
ASA 5505	Use one of the following: • AnyConnect Premium license: – Base license or Security Plus license: 2 sessions. – *Optional permanent or time-based licenses: 10 or 25 sessions.* – *Shared licenses are not supported.*[3] • AnyConnect Essentials license[4]: 25 sessions.
ASA 5512-X	Use one of the following: • AnyConnect Premium license: – Base license: 2 sessions. – *Optional permanent or time-based licenses: 10, 25, 50, 100, or 250 sessions.* – *Optional Shared licenses*[3]*: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.* • AnyConnect Essentials license[4]: 250 sessions.
ASA 5515-X	Use one of the following: • AnyConnect Premium license: – Base license: 2 sessions. – *Optional permanent or time-based licenses: 10, 25, 50, 100, or 250 sessions.* – *Optional Shared licenses*[3]*: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.* • AnyConnect Essentials license[4]: 250 sessions.
ASA 5525-X	Use one of the following: • AnyConnect Premium license: – Base license: 2 sessions. – *Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, or 750 sessions.* – *Optional Shared licenses*[3]*: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.* • AnyConnect Essentials license[4]: 750 sessions.

Model	License Requirement[1,2]
ASA 5545-X	Use one of the following: • AnyConnect Premium license: – Base license: 2 sessions. – *Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, or 2500 sessions.* – *Optional Shared licenses[3]: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.* • AnyConnect Essentials license[4]: 2500 sessions.
ASA 5555-X	Use one of the following: • AnyConnect Premium license: – Base license: 2 sessions. – *Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, 2500, or 5000 sessions.* – *Optional Shared licenses[3]: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.* • AnyConnect Essentials license[4]: 5000 sessions.
ASA 5585-X with SSP-10	Use one of the following: • AnyConnect Premium license: – Base license: 2 sessions. – *Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, 2500, or 5000 sessions.* – *Optional Shared licenses[3]: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.* • AnyConnect Essentials license[4]: 5000 sessions.
ASA 5585-X with SSP-20, -40, and -60	Use one of the following: • AnyConnect Premium license: – Base license: 2 sessions. – *Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, 2500, 5000, or 10000 sessions.* – *Optional Shared licenses[3]: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.* • AnyConnect Essentials license[4]: 10000 sessions.

Model	License Requirement[1,2]
ASASM	Use one of the following: • AnyConnect Premium license: – Base license: 2 sessions. – *Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, 2500, 5000, or 10000 sessions.* – *Optional Shared licenses[3]: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.* • AnyConnect Essentials license[4]: 10000 sessions.
ASAv with 1 Virtual CPU	• Standard license: 2 sessions. • Premium license: 250 sessions.
ASAv with 4 Virtual CPUs	• Standard license: 2 sessions. • Premium license: 750 sessions.

1. If you start a clientless SSL VPN session and then start an AnyConnect client session from the portal, 1 session is used in total. However, if you start the AnyConnect client first (from a standalone client, for example) and then log into the clientless SSL VPN portal, then 2 sessions are used.
2. The maximum combined VPN sessions of *all* types cannot exceed the maximum sessions shown in this table. For the ASA 5505, the maximum combined sessions is 10 for the Base license, and 25 for the Security Plus license.
3. A shared license lets the ASA act as a shared license server for multiple client ASAs. The shared license pool is large, but the maximum number of sessions used by each individual ASA cannot exceed the maximum number listed for permanent licenses.
4. The AnyConnect Essentials license enables AnyConnect VPN client access to the ASA. This license does not support browser-based SSL VPN access or Cisco Secure Desktop. For these features, activate an AnyConnect Premium license instead of the AnyConnect Essentials license.

   Note: With the AnyConnect Essentials license, VPN users can use a Web browser to log in, and download and start (WebLaunch) the AnyConnect client.

   The AnyConnect client software offers the same set of client features, whether it is enabled by this license or an AnyConnect Premium SSL VPN Edition license.

   The AnyConnect Essentials license cannot be active at the same time as the following licenses on a given ASA: AnyConnect Premium license (all types) or the Advanced Endpoint Assessment license. You can, however, run AnyConnect Essentials and AnyConnect Premium licenses on different ASAs in the same network.

   By default, the ASA uses the AnyConnect Essentials license, but you can disable it to use other licenses by using the **no anyconnect-essentials** command.

   For a detailed list of the features supported by the AnyConnect Essentials license and AnyConnect Premium license, see *AnyConnect Secure Mobility Client Features, Licenses, and OSs*:

   http://www.cisco.com/en/US/products/ps10884/products_feature_guides_list.html

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Remote PC System Requirements

For the requirements of endpoint computers running the AnyConnect Secure Mobility Client, see the release notes for the AnyConnect client version you are deploying with the ASA.

Remote HTTPS Certificates Limitation

The ASA does not verify remote HTTPS certificates.

Configuring AnyConnect Connections

This section describes prerequisites, restrictions, and detailed tasks to configure the ASA to accept AnyConnect VPN client connections.

Configuring the ASA to Web-Deploy the Client

The section describes the steps to configure the ASA to web-deploy the AnyConnect client.

Prerequisites

Copy the client image package to the ASA using TFTP or another method.

Detailed Steps

	Command	Purpose
Step 1	`anyconnect image` *`filename order`* **Example:** `hostname(config-webvpn)#`**`anyconnect image anyconnect-win-2.3.0254-k9.pkg 1`** `hostname(config-webvpn)#`**`anyconnect image anyconnect-macosx-i386-2.3.0254-k9.pkg 2`** `hostname(config-webvpn)#`**`anyconnect image anyconnect-linux-2.3.0254-k9.pkg 3`**	Identifies a file on flash as an AnyConnect client package file. The ASA 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 ASA 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. **Note** You must issue the **anyconnect enable** command after configuring the AnyConnect images with the **anyconnect image xyz** command. If you do not enable the **anyconnect enable** command, AnyConnect will not operate as expected, and **show webvpn anyconnect** considers the SSL VPN client as not enabled rather than listing the installed AnyConnect packages.
Step 2	**`enable`** *`interface`* **Example:** `hostname(config)#` **`webvpn`** `hostname(config-webvpn)#` **`enable outside`**	Enables SSL on an interface for clientless or AnyConnect SSL connections.
Step 3	**`anyconnect enable`**	Without issuing this command, AnyConnect does not function as expected, and a **show webvpn anyconnect** command returns that the "SSL VPN is not enabled," instead of listing the installed AnyConnect packages.

	Command	Purpose
Step 4	**ip local pool** *poolname startaddr-endaddr* **mask** *mask* **Example:** hostname(config)# **ip local pool vpn_users 209.165.200.225-209.165.200.254 mask 255.255.255.224**	(Optional) Creates an address pool. You can use another method of address assignment, such as DHCP and/or user-assigned addressing.
Step 5	**address-pool** *poolname* **Example:** hostname(config)# **tunnel-group telecommuters general-attributes** hostname(config-tunnel-general)# **address-pool vpn_users**	Assigns an address pool to a tunnel group.
Step 6	**default-group-policy** *name* **Example:** hostname(config-tunnel-general)# **default-group-policy sales**	Assigns a default group policy to the tunnel group.
Step 7	**group-alias** *name* **enable** **Example:** hostname(config)# **tunnel-group telecommuters webvpn-attributes** hostname(config-tunnel-webvpn)# **group-alias sales_department enable**	Enables the display of the tunnel-group list on the clientless portal and AnyConnect GUI login page. The list of aliases is defined by the *group-alias name enable* command.
Step 8	**tunnel-group-list enable** **Example:** hostname(config)# **webvpn** hostname(config-webvpn)# **tunnel-group-list enable**	Specifies the AnyConnect clients as a permitted VPN tunneling protocol for the group or user.
Step 9	**vpn-tunnel-protocol** **Example:** hostname(config)# **group-policy sales attributes** hostname(config-group-policy)# **webvpn** hostname(config-group-webvpn)# **vpn-tunnel-protocol**	Specifies SSL as a permitted VPN tunneling protocol for the group or user. You can also specify additional protocols. For more information, see the **vpn-tunnel-protocol** command in the command reference. For more information about assigning users to group policies, see Chapter 6, Configuring Connection Profiles, Group Policies, and Users.

Enabling Permanent Client Installation

Enabling permanent client installation 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.

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

anyconnect keep-installer installer

The default is that permanent installation of the client is enabled. The client remains on the remote computer at the end of the session. The following example configures the existing group-policy *sales* to remove the client on the remote computer at the end of the session:

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

Configuring DTLS

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.

By default, DTLS is enabled when SSL VPN access is enabled on an interface. If you disable DTLS, SSL VPN connections connect with an SSL VPN tunnel only.

Note In order for DTLS to fall back to a TLS connection, Dead Peer Detection (DPD) must be enabled. If you do not enable DPD, and the DTLS connection experiences a problem, the connection terminates instead of falling back to TLS. For more information on enabling DPD, see Enabling and Adjusting Dead Peer Detection, page 11-15

You can disable DTLS for all AnyConnect client users with the **enable** command **tls-only** option in webvpn configuration mode:

enable <*interface*> **tls-only**

For example:

hostname(config-webvpn)# **enable outside tls-only**

By default, DTLS is enabled for specific groups or users with the **anyconnect ssl dtls** command in group policy webvpn or username webvpn configuration mode:

[**no**] **anyconnect ssl dtls {enable interface | none}**

If you need to disable DTLS, use the **no** form of the command. For example:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# no anyconnect ssl dtls none
```

Prompting Remote Users

You can enable the ASA to prompt remote SSL VPN client users to download the client with the **anyconnect ask** command from group policy webvpn or username webvpn configuration modes:

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

anyconnect enable prompts the remote user to download the client or go to the clientless portal page and waits indefinitely for user response.

anyconnect ask enable default immediately downloads the client.

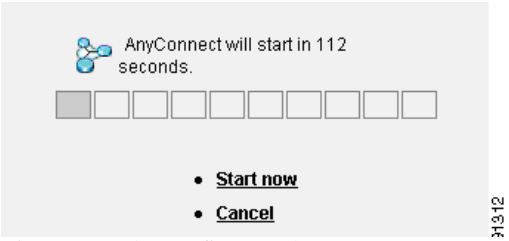
anyconnect ask enable default webvpn immediately goes to the portal page.

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

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

Figure 11-1 shows the prompt displayed to remote users when either **default anyconnect timeout** *value or* **default webvpn timeout** *value is configured:*

Figure 11-1 Prompt Displayed to Remote Users for SSL VPN Client Download



The following example configures the ASA to prompt the user to download the client or go to the clientless portal page and wait *10 seconds for a response* before downloading the client:

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

Enabling AnyConnect Client Profile Downloads

You enable Cisco AnyConnect Secure Mobility client features in the AnyConnect profiles—XML files that contain configuration settings for the core client with its VPN functionality and for the optional client modules Network Access Manager (NAM), posture, telemetry, and Web Security. The ASA deploys the profiles during AnyConnect installation and updates. Users cannot manage or modify profiles.

Profile Editor in ASDM

You can configure a profile using the AnyConnect profile editor, a convenient GUI-based configuration tool launched from ASDM. The AnyConnect software package for Windows, version 2.5 and later, includes the editor, which activates when you load the AnyConnect package on the ASA and specify it as an AnyConnect client image.

Standalone Profile Editor

We also provide a standalone version of the profile editor for Windows that you can use as an alternative to the profile editor integrated with ASDM. If you are predeploying the client, you can use the standalone profile editor to create profiles for the VPN service and other modules that you deploy to computers using your software management system. For more information about using the profile editor, see the Cisco AnyConnect Secure Mobility Client Administrator Guide.

Note The AnyConnect client protocol defaults to SSL. To enable IPsec IKEv2, you must configure the IKEv2 settings on the ASA and also configure IKEv2 as the primary protocol in the client profile. The IKEv2enabled profile must be deployed to the endpoint computer, otherwise the client attempts to connect using SSL. For more information, see the Cisco AnyConnect Secure Mobility Client Administrator Guide.

Follow these steps to edit a profile and enable the ASA to download it to remote clients:

Step 1 Use the profile editor from ASDM or the standalone profile editor to create a profile. For more information, see the Cisco AnyConnect Secure Mobility Client Administrator Guide.

Step 2 Load the profile file into flash memory on the ASA using tftp or another method.

Step 3 Use the **anyconnect profiles** command from webvpn configuration mode to identify the file as a client profile to load into cache memory.

The following example specifies the files *sales_hosts.xml* and *engineering_hosts.xml* as profiles:

```
asa1(config-webvpn)# anyconnect profiles sales disk0:/sales_hosts.xml
asa1(config-webvpn)# anyconnect profiles engineering disk0:/engineering_hosts.xml
```

The profiles are now available to group policies.

You can view the profiles loaded in cache memory using the **dir cache:stc/profiles** command:

```
hostname(config-webvpn)# dir cache:/stc/profiles

Directory of cache:stc/profiles/

0      ----  774         11:54:41 Nov 22 2006  engineering.xml
0      ----  774         11:54:29 Nov 22 2006  sales.xml

2428928 bytes total (18219008 bytes free)
hostname(config-webvpn)#
```

Step 4 Enter group policy webvpn configuration mode and specify a client profile for a group policy with the **anyconnect profiles** command:

You can enter the **anyconnect profiles value** command followed by a question mark (**?**) to view the available profiles. For example:

```
asa1(config-group-webvpn)# anyconnect profiles value ?

config-group-webvpn mode commands/options:
Available configured profile packages:
  engineering
  sales
```

The next example configures the group policy to use the profile *sales* with the client profile type *vpn*:

```
asa1(config-group-webvpn)# anyconnect profiles value sales type vpn
asa1(config-group-webvpn)#
```

Enabling AnyConnect Client Deferred Upgrade

Deferred Upgrade allows the AnyConnect user to delay download of a client upgrade. When a client update is available, AnyConnect opens a dialog asking the user if they would like to update, or to defer the upgrade.

Deferred Upgrade is enabled by adding custom attributes to the ASA, and then referencing and configuring those attributes in a group policy.

The following custom attributes support Deferred Upgrade:

Table 11-1 Custom Attributes for Deferred Upgrade

Custom Attribute	Valid Values	Default Value	Notes
DeferredUpdateAllowed	true false	false	True enables deferred update. If deferred update is disabled (false), the settings below are ignored.
DeferredUpdateMinimumVersion	x.y.z	0.0.0	Minimum version of AnyConnect that must be installed for updates to be deferrable. The minimum version check applies to all modules enabled on the headend. If any enabled module (including VPN) is not installed or does not meet the minimum version, then the connection is not eligible for deferred update. If this attribute is not specified, then a deferral prompt is displayed (or auto-dismissed) regardless of the version installed on the endpoint.
DeferredUpdateDismissTimeout	0-300 (seconds)	none (disabled)	Number of seconds that the deferred upgrade prompt is displayed before being dismissed automatically. This attribute only applies when a deferred update prompt is to be displayed (the minimum version attribute is evaluated first). If this attribute is missing, then the auto-dismiss feature is disabled, and a dialog is displayed (if required) until the user responds. Setting this attribute to zero allows automatic deferral or upgrade to be forced based on: • The installed version and the value of DeferredUpdateMinimumVersion. • The value of DeferredUpdateDismissResponse.
DeferredUpdateDismissResponse	defer update	update	Action to take when DeferredUpdateDismissTimeout occurs.

Step 1 Create the custom attributes with the **anyconnnect-custom-attr** command in webvpn configuration mode:

[no] anyconnect-custom-attr *attr-name* **[description** *description***]**

The following example shows how to add the custom attribute DeferredUpdateAllowed:

```
hostname(config)# webvpn
hostame(config-webvpn)# anyconnect-custom-attr DeferredUpdateAllowed description
"Indicates if the deferred update feature is enabled or not"
```

Step 2 Add or remove the custom attributes to a group policy, and configure values for each attribute, using the **anyconnect-custom** command:

anyconnect-custom *attr-name* **value** *value*

no anyconnect-custom *attr-nam*

The following example shows how to enable Deferred Update for the group policy named sales:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-policy)# anyconnect-custom DeferredUpdateAllowed value true
```

Enabling Additional AnyConnect Client Features

To minimize download time, the client only requests downloads (from the ASA) of the core modules that it needs. As additional features become available for the AnyConnect client, you need to update the remote clients in order for them to use the features.

To enable new features, you must specify the new module names using the **anyconnect modules** command from group policy webvpn or username webvpn configuration mode:

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

Separate multiple strings with commas.

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

Enabling Start Before Logon

Start Before Logon (SBL) allows login scripts, password caching, drive mapping, and more, for the AnyConnect client installed on a Windows PC. For SBL, you must enable the ASA to download the module which enables graphical identification and authentication (GINA) for the AnyConnect client. The following procedure shows how to enable SBL:

Step 1 Enable the ASA to download the GINA module for VPN connection to specific groups or users using the **anyconnect modules** *vpngina* command from group policy webvpn or username webvpn configuration modes.

In the following example, the user enters group-policy attributes mode for the group policy *telecommuters*, enters webvpn configuration mode for the group policy, and specifies the string *vpngina*:

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

Step 2 Retrieve a copy of the client profiles file (AnyConnectProfile.tmpl).

Step 3 Edit the profiles file to specify that SBL is enabled. The example below shows the relevant portion of the profiles file (AnyConnectProfile.tmpl) for Windows:

```
<Configuration>
    <ClientInitialization>
        <UseStartBeforeLogon>false</UseStartBeforeLogon>
    </ClientInitialization>
```

The <UseStartBeforeLogon> tag determines whether the client uses SBL. To turn SBL on, replace *false* with *true*. The example below shows the tag with SBL turned on:

```
    <ClientInitialization>
        <UseStartBeforeLogon>true</UseStartBeforeLogon>
    </ClientInitialization>
```

Step 4 Save the changes to AnyConnectProfile.tmpl and update the profile file for the group or user on the ASA using the **profile** command from webvpn configuration mode. For example:

```
asa1(config-webvpn)#anyconnect profiles sales disk0:/sales_hosts.xml
```

Translating Languages for AnyConnect User Messages

The ASA provides language translation for the portal and screens displayed to users that initiate browser-based, Clientless SSL VPN connections, as well as the interface displayed to Cisco AnyConnect VPN Client users.

This section describes how to configure the ASA to translate these user messages and includes the following sections:

- Understanding Language Translation, page 11-12
- Creating Translation Tables, page 11-12

Understanding Language Translation

Functional areas and their messages that are visible to remote users are organized into translation domains. All *messages displayed on the user interface of the Cisco AnyConnect VPN Client are located in the AnyConnect domain.*

The software image package for the ASA includes a translation table template for the AnyConnect domain. You can export the template, which creates an XML file of the template at the URL you provide. The message fields in this file are empty. You can edit the messages and import the template to create a new translation table object that resides in flash memory.

You can also export an existing translation table. The XML file created displays the messages you edited previously. Reimporting this XML file with the same language name creates an new version of the translation table object, overwriting previous messages. Changes to the translation table for the AnyConnect domain are immediately visible to AnyConnect client users.

Creating Translation Tables

The following procedure describes how to create translation tables for the AnyConnect domain:

Step 1 Export a translation table template to a computer with the **export webvpn translation-table** command from privileged EXEC mode.

In the following example, the **show webvpn translation-table** command shows available translation table templates and tables.

```
hostname# show import webvpn translation-table
Translation Tables' Templates:
customization
AnyConnect
CSD
PortForwarder
url-list
webvpn
Citrix-plugin
RPC-plugin
Telnet-SSH-plugin
VNC-plugin

Translation Tables:
```

Then the user exports the translation table for the AnyConnect translation domain. The filename of the XML file created is named *client* and contains empty message fields:

```
hostname# export webvpn translation-table AnyConnect template
tftp://209.165.200.225/client
```

In the next example, the user exports a translation table named *zh*, which was previously imported from a template. zh is the abbreviation by Microsoft Internet Explorer for the Chinese language.

```
hostname# export webvpn translation-table customization language zh
tftp://209.165.200.225/chinese_client
```

Step 2 Edit the Translation Table XML file. The following example shows a portion of the AnyConnect template. The end of this output includes a message ID field (msgid) and a message string field (msgstr) for the message *Connected*, which is displayed on the AnyConnect client GUI when the client establishes a VPN connection. The complete template contains many pairs of message fields:

```
# SOME DESCRIPTIVE TITLE.
# Copyright (C) YEAR THE PACKAGE'S COPYRIGHT HOLDER
# This file is distributed under the same license as the PACKAGE package.
# FIRST AUTHOR <EMAIL@ADDRESS>, YEAR.
#
#, fuzzy
msgid ""
msgstr ""
"Project-Id-Version: PACKAGE VERSION\n"
"Report-Msgid-Bugs-To: \n"
"POT-Creation-Date: 2006-11-01 16:39-0700\n"
"PO-Revision-Date: YEAR-MO-DA HO:MI+ZONE\n"
"Last-Translator: FULL NAME <EMAIL@ADDRESS>\n"
"Language-Team: LANGUAGE <LL@li.org>\n"
"MIME-Version: 1.0\n"
"Content-Type: text/plain; charset=CHARSET\n"
"Content-Transfer-Encoding: 8bit\n"

#: C:\cygwin\home\<user>\cvc\main\Api\AgentIfc.cpp:23
#: C:\cygwin\home\<user>\cvc\main\Api\check\AgentIfc.cpp:22
#: C:\cygwin\home\<user>\cvc\main\Api\save\AgentIfc.cpp:23
#: C:\cygwin\home\<user>\cvc\main\Api\save\AgentIfc.cpp~:20
#: C:\cygwin\home\<user>\cvc\main\Api\save\older\AgentIfc.cpp:22
msgid "Connected"
msgstr ""
```

The msgid contains the default translation. The msgstr that follows msgid provides the translation. To create a translation, enter the translated text between the quotes of the msgstr string. For example, to translate the message “Connected” with a Spanish translation, insert the Spanish text between the quotes:

```
msgid "Connected"
msgstr "Conectado"
```

Be sure to save the file.

Step 3 Import the translation table using the **import webvpn translation-table** command from privileged EXEC mode. Be sure to specify the name of the new translation table with the abbreviation for the language that is compatible with the browser.

In the following example, the XML file is imported *es-us*—the abbreviation used by Microsoft Internet Explorer for Spanish spoken in the United States.

```
hostname# import webvpn translation-table AnyConnect language es-us
tftp://209.165.200.225/client
hostname# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
hostname# show import webvpn translation-table
```

```
Translation Tables' Templates:
AnyConnect
PortForwarder
csd
customization
keepout
url-list
webvpn
Citrix-plugin
RPC-plugin
Telnet-SSH-plugin
VNC-plugin

Translation Tables:
es-us AnyConnect
```

Configuring Advanced AnyConnect SSL Features

The following section describes advanced features that fine-tune AnyConnect SSL VPN connections, and includes the following sections:

- Enabling Rekey, page 11-14
- Enabling and Adjusting Dead Peer Detection, page 11-15
- Enabling Keepalive, page 11-15
- Using Compression, page 11-16
- Adjusting MTU Size, page 11-17
- Updating AnyConnect Client Images, page 11-17

Enabling Rekey

When the ASA and the AnyConnect client client perform a rekey on an SSL VPN connection, 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 **anyconnect ssl rekey** command from group-policy or username webvpn modes.

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

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

method ssl specifies that the client estanyablishes a new tunnel during rekey.

method none disables rekey.

Note Configuring the rekey method as **ssl** or **new-tunnel** specifies that the client establishes a new tunnel during rekey instead of the SSL renegotiation taking place during the rekey. See the command reference for a history of the **anyconnect ssl rekey** command.

time *minutes* specifies the number of minutes from the start of the session, or from the last rekey, until the 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-webvpn)# anyconnect ssl rekey method ssl
hostname(config-group-webvpn)# anyconnect ssl rekey time 30
```

Enabling and Adjusting Dead Peer Detection

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

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

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

Where:

gateway seconds enables DPD performed by the ASA (gateway) and specifies the frequency, from 5 to 3600 seconds, with which the ASA (gateway) performs DPD.

gateway none disables DPD performed by the ASA.

client *seconds* enable DPD performed by the client, and specifies the frequency, from 5 to 3600 seconds, with which the client performs DPD.

client none disables DPD performed by the client.

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

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

Note If you enable DTLS, enable Dead Peer Detection (DPD) also. DPD enables a failed DTLS connection to fallback to TLS. Otherwise, the connection terminates.

The following example sets the frequency of DPD performed by the ASA 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-webvpn)# anyconnect dpd-interval gateway 30
hostname(config-group-webvpn)# anyconnect dpd-interval client 10
```

Enabling Keepalive

You can adjust the frequency of keepalive messages to ensure that an 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.

Note Keepalives are enabled by default. If you disable keepalives, in the event of a failover event, SSL VPN client sessions are not carried over to the standby device.

To set the frequency of keepalive messages, use the **keepalive** command from group-policy webvpn or username webvpn configuration mode:

[no] anyconnect ssl 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 enabled.

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 ASA 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)#anyconnect ssl keepalive 300
```

Using Compression

Compression increases the communications performance between the ASA and the client by reducing the size of the packets being transferred for low-bandwidth connections. By default, compression for all SSL VPN connections is enabled on the ASA, both at the global level and for specific groups or users.

Note When implementing compression on broadband connections, you must carefully consider the fact that compression relies on loss-less connectivity. This is the main reason that it is not enabled by default on broadband connections.

Compression must be turned-on globally using the **anyconnect ssl compression** command from global configuration mode, and then it can be set for specific groups or users with the **anyconnect ssl compression** command in group-policy and username webvpn modes.

Changing Compression Globally

To change the global compression settings, use the **anyconnect ssl compression** command from global configuration mode:

compression

no compression

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
```

Changing Compression for Groups and Users

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

anyconnect ssl compression {**deflate | none**}

no anyconnect ssl compression {**deflate | none**}

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

To remove the **anyconnect ssl 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, compression is disabled for the group-policy sales:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# no anyconnect ssl compression none
```

Adjusting MTU Size

You can adjust the MTU size (from 256 to 1406 bytes) for SSL VPN connections established by the client with the **anyconnect mtu** command from group policy webvpn or username webvpn configuration mode:

[no]anyconnect mtu *size*

This command affects only the AnyConnect client. The legacy Cisco SSL VPN Client () is not capable of adjusting to different MTU sizes.

The default for this command in the default group policy is **no anyconnect mtu**. The MTU size is adjusted automatically based on the MTU of the interface that the connection uses, minus the IP/UDP/DTLS overhead.

This command affects client connections established in SSL and those established in SSL with DTLS.

Examples The following example configures the MTU size to 1200 bytes for the group policy *telecommuters*:

```
hostname(config)# group-policy telecommuters attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)#anyconnect mtu 1200
```

Updating AnyConnect Client Images

You can update the client images on the ASA at any time using the following procedure:

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

Step 2 If the new clientt image files have the same filenames as the files already loaded, reenter the **anyconnect image** command that is in the configuration. If the new filenames are different, uninstall the old files using the **noanyconnect image** command. Then use the **anyconnect image** command to assign an order to the images and cause the ASA to load the new images.

Enabling IPv6 VPN Access

If you want to configure IPv6 access, you must use the command-line interface. Release 9.0(x) of the ASA adds support for IPv6 VPN connections to its outside interface using SSL and IKEv2/IPsec protocols.

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 IPv6 address assignment):

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

Note You can configure the ASA to assign an IPv4 address, an IPv6 address, or both an IPv4 and an IPv6 address to an AnyConnect client by creating internal pools of addresses on the ASA or by assigning a dedicated address to a local user on the ASA.

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 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
```

Monitoring AnyConnect Connections

To view information about active sessions use the **show vpn-sessiondb**:

Command	Purpose
`show vpn-sessiondb`	Displays information about active sessions.
`vpn-sessiondb logoff`	Logs off VPN sessions.

Command	Purpose
show vpn-sessiondb anyconnect	Enhances the VPN session summary to show OSPFv3 session information.
show vpn-sessiondb ratio encryption	Shows the number of tunnels and percentages for the Suite B algorithms (such as AES-GCM-128, AES-GCM-192, AES-GCM-256, AES-GMAC-128, and so on).

Examples

The Inactivity field shows the elapsed time since an AnyConnect session lost connectivity. If the session is active, 00:00m:00s appears in this field.

```
hostname# show vpn-sessiondb

Session Type: SSL VPN Client

Username     : lee
Index        : 1                      IP Addr      : 209.165.200.232
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  : Internet Explorer
Group        : DfltGrpPolicy
Login Time   : 14:32:03 UTC Wed Mar 20 2007
Duration     : 0h:00m:04s
Inactivity   : 0h:00m:04s
Filter Name  :

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

hostname# vpn-sessiondb logoff name tester
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions with name "tester" logged off : 1
```

Logging Off AnyConnect VPN Sessions

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

vpn-sessiondb logoff

The following example logs off all VPN sessions:

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

You can log off individual sessions using either the name argument or the index argument:

vpn-session-db logoff name *name*

vpn-session-db logoff index *index*

The sessions that have been inactive the longest time are marked as idle (and are automatically logged off) so that license capacity is not reached and new users can log in. If the session resumes at a later time, it is removed from the inactive list.

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

```
hostname# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : lee                    Index        : 1
Assigned IP  : 192.168.246.1           Public IP    : 10.139.1.2
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 11079                  Bytes Rx     : 4942
Group Policy : EngPolicy            Tunnel Group : EngGroup
Login Time   : 15:25:13 EST Fri Jan 28 2011
Duration     : 0h:00m:15s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

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

```
hostname# vpn-sessiondb logoff name lee
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions with name “lee” logged off : 1

hostname#
```

Configuration Examples for Enabling AnyConnect Connections

The following example shows how to configure L2TP over IPsec:

```
ip local pool sales_addresses 209.165.202.129-209.165.202.158
aaa-server sales_server protocol radius
crypto ipsec transform-set sales_l2tp_transform esp-3des esp-sha-hmac
crypto ipsec transform-set sales_l2tp_transform mode transport
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
l2tp tunnel hello 100

group-policy sales_policy internal
group-policy sales_policy attributes
 wins-server value 209.165.201.3 209.165.201.4
 dns-server value 209.165.201.1 209.165.201.2
 vpn-tunnel-protocol l2tp-ipsec
tunnel-group sales_tunnel type remote-access
tunnel-group sales_tunnel general-attributes
 address-pool sales_addresses
 authentication-server-group none
 accounting-server-group sales_server
 default-group-policy sales_policy
tunnel-group sales_tunnel ppp-attributes
 authentication pap
```

Feature History for AnyConnect Connections

Table 11-2 lists the release history for this feature.

Table 11-2 Feature History for AnyConnect Connections

Feature Name	Releases	Feature Information
AnyConnect Connections	7.2(1)	The following commands were introduced or modified: **authentication eap-proxy**, **authentication ms-chap-v1**, **authentication ms-chap-v2**, **authentication pap**, **l2tp tunnel hello**, **vpn-tunnel-protocol l2tp-ipsec**.
IPsec IKEv2	8.4(1)	IKEv2 was added to support IPsec IKEv2 connections for AnyConnect and LAN-to-LAN.