CHAPTER 2

Common AnyConnect VPN Client Installation and Configuration Procedures

Installing the AnyConnect Client

The installation and configuration consists of two parts: what you have to do on the security appliance and what you have to do on the remote PC. The AnyConnect client software part of the ASA Release 8.0(1) and later and ASDM Release 6.0 and later. You can decide whether to make the AnyConnect client software permanently resident on the remote PC, or whether to have it resident only for the duration of the connection.

This chapter contains procedures for installing the AnyConnect client software on the ASA5500 using the Adaptive Security Device Manager (ASDM) or the CLI command interface. It also describes how to install the AnyConnect client on a user's PC and how to enable AnyConnect client features after installation.

WebLaunch Mode

Without a previously-installed client, remote users enter into their browser the IP address or DNS name of an interface configured to accept clientless SSL VPN connections. Unless the security appliance is configured to redirect http:// requests to https://, users must enter the URL in the form https://<*address*>.

Note A user with a clientless SSL VPN connection can switch to an AnyConnect client SSL VPN connection by clicking the AnyConnect drawer on the portal and following the instructions on that page.

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

Standalone Mode

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

When the client negotiates an SSL VPN connection with the security appliance, it connects using Transport Layer Security (TLS). The client can also negotiate a simultaneous Datagram Transport Layer Security (DTLS) connection. 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 security appliance, or it can be installed manually on the remote PC by the system administrator. This document contains information about how to configure the features of the AnyConnect client. For more detailed information about configuring the AnyConnect client and other SSL VPN connections on the security appliance, see "Configuring SSL VPN Connections" in *Cisco Security Appliance Command Line Configuration Guide*. For detailed descriptions of the commands referred to in this administrator's guide, see the *Cisco ASA 5500 Command Reference Guide* for version 8.0 or later.

The security appliance loads the client based on the group policy or username attributes of the user establishing the connection. You can configure the security appliance 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 security appliance to either download the client after a timeout period or present the portal page.

Note When using Start Before Logon, the VPN Gina (VPN Graphical Identification and Authentication) a cannot be installed dynamically if the AnyConnect client is installed manually. The VPN Gina can be installed either before or after the AnyConnect client, but they must either be both installed manually or both installed dynamically (CSCsh38590).

This section describes installation-specific issues and procedures for the AnyConnect client Release 2.0(1), and contains the following sections:

- Before You Install the AnyConnect Client, page 2-2
- Installing the AnyConnect Client on a User's PC, page 2-8
- Installing the AnyConnect Client on a User's PC, page 2-8

Before You Install the AnyConnect Client

The following sections contain recommendations to ensure successful AnyConnect client installation, as well as tips about certificates, Cisco Security Agent (CSA), adding trusted sites, and responding to browser alerts:

- Ensuring Automatic Installation of AnyConnect Clients, page 2-2
- AnyConnect Client and New Windows Installations, page 2-3
- Adding a Security Appliance to the List of Trusted Sites (Internet Explorer), page 2-3
- Adding a Security Certificate in Response to Browser Security Alert Windows, page 2-4

Ensuring Automatic Installation of AnyConnect Clients

The following recommendations and caveats apply to the automatic installation of AnyConnect client software on client PCs:

- To minimize user prompts during AnyConnect client setup, make sure certificate data on client PCs and on the security appliance match:
  - If you are using a Certificate Authority (CA) for certificates on the security appliance, choose one that is already configured as a trusted CA on client machines.
  - If you are using a self-signed certificate on the security appliance, be sure to install it as a trusted root certificate on clients.

The procedure varies by browser. See the procedures that follow this section.

- Make sure the Common Name (CN) in security appliance certificates matches the name clients use to connect to it. By default, the security appliance certificate CN field is its IP address. If clients use a DNS name, change the CN field on the security appliance certificate to that name.

- The Cisco Security Agent (CSA) might display warnings during the AnyConnect client installation.

Current shipping versions of CSA do not have a built-in rule that is compatible with the AnyConnect client. You can create the following rule using CSA version 5.0 or later by following these steps:

Step 1 In the Rule Module: "Cisco Secure Tunneling Client Module", add a FACL:

```
Priority Allow, no Log, Description: "Cisco Secure Tunneling Browsers, read/write
vpnweb.ocx"
Applications in the following class: "Cisco Secure Tunneling Client - Controlled Web
Browsers"
Attempt: Read file, Write File
```

On any of these files: @SYSTEM\vpnweb.ocx

Step 2 Application Class: "Cisco Secure Tunneling Client - Installation Applications" add the following process names:

```
**\vpndownloader.exe
@program_files\**\Cisco\Cisco AnyConnect VPN Client\vpndownloader.exe
```

This rule will be built in to a future release of CSA.

- We recommend that Microsoft Internet Explorer (MSIE) users add the security appliance to the list of trusted sites, or install Java. Doing so enables the ActiveX control to install with minimal interaction from the user. This is particularly important for users of Windows XP SP2 with enhanced security. Windows Vista users *must* add the security appliance to the list of trusted sites in order to use the dynamic deployment feature. Refer to the following sections for instructions.

AnyConnect Client and New Windows Installations

In rare circumstances, if you install the AnyConnect client on a computer that has a new or clean Windows installation, the AnyConnect client might fail to connect, and your computer might display the following message:

`The required system DLL (filename) is not present on the system.`

This could occur if the computer does not have the file MSVCP60.dll or MSVCRT.dll located in the winnt\system32 directory. For more information about this problem, see the Microsoft Knowledge Base, article 259403, at http://support.microsoft.com/kb/259403.

Adding a Security Appliance to the List of Trusted Sites (Internet Explorer)

To add a security appliance to the list of trusted sites, use Microsoft Internet Explorer and do the following steps.

Note Adding a security appliance to the list of trusted sites for Internet Explorer is required for those running Windows Vista who want to use WebLaunch.

Step 1 Go to Tools > Internet Options > Trusted Sites.

The Internet Options window opens.

Step 2 Click the Security tab.

Step 3 Click the Trusted Sites icon.

Step 4 Click Sites.

The Trusted Sites window opens.

Step 5 Type the host name or IP address of the security appliance. Use a wildcard such as https://*.yourcompany.com to allow all ASA 5500s within the yourcompany.com domain to be used to support multiple sites.

Step 6 Click Add.

Step 7 Click OK.

The Trusted Sites window closes.

Step 8 Click OK in the Internet Options window.

Note To use Microsoft Active Directory to add the security appliance to the list of Internet Explorer trusted sites for domain users, see Using Microsoft Active Directory to Add the Security Appliance to the List of Internet Explorer Trusted Sites for Domain Users, page B-1.

When a user gets the server certificate for the security appliance from a globally trusted certificate authority—for example, Verisign or Cisco—the user never sees a Security Alert pop-up when connecting to that security appliance.

Adding a Security Certificate in Response to Browser Security Alert Windows

This section explains how to install a self-signed certificate as a trusted root certificate on a client in response to the browser alert windows.

Connecting to this security appliance.

A remote user using standalone mode might see a Security Alert dialog box in several possible login situations. The following examples and scenarios show some instances. After these descriptions, you'll see how to add a security certificate to avoid these situations.

The following examples illustrate sequences of events involving the pop-up Security Alert dialog box.

Example Set 1

1. A user connects to badly configured security appliance #1. As a result, the user sees the pop-up Security Alert dialog box.
2. The user approves the certificate.

3. The user connects successfully to security appliance #1.
4. The user disconnects from security appliance #1.
5. The user reconnects to badly configured security appliance #1.
6. The user does not see the pop-up dialog box, because the certificate is stored in the preferences file. The user connects successfully to security appliance #1.
7. The user disconnects from security appliance #1.
8. The user connects to correctly configured security appliance #2.
9. The user sees no dialog box and connects successfully.
10. The user disconnects from security appliance #2.
11. The user connects to badly configured security appliance #1.
12. The user sees a pop-up Security Alert dialog box prompt.

Example Set 2

The following are examples of non-serious errors that result in a Security Alert dialog box prompting the user.

- Invalid Common Name: The hostname in the certificate sent to us from the security appliance does not match the hostname that the user connected to.

  For example, the user connects to 10.94.147.93, and the certificate received from the security appliance contains cvc-asa06.cisco.com. 10.94.147.93 and cvc-asa06.cisco.com might or might not be the same machine. The Security Alert dialog box prompts the user to approve or disapprove the certificate.
- Invalid Date: The certificate received from the security appliance has expired or is not yet valid. This could be because the date on the customer's machine is incorrect or because the certificate really is invalid. The Security Alert dialog box prompts the user to approve or disapprove the certificate.
- Invalid Certificate Authority: The certificate received from the security appliance has been signed by a Certificate Authority that is not recognized by the AnyConnect client. The AnyConnect client prompts the user for approval/disapproval. Recommendation: The root certificate (certificate of the Certificate Authority) should be imported into the client machine out of band (via E-mail, website, floppy disk, CD, and so on).

Example Set 3

The following are examples of serious errors that result in no Security Alert prompt and no connection.

- Certificate cannot be read.
- Bad password.
- Certificate not sent to the client.
- Bad Usage: Certificate received from the security appliance was not meant to be used as a server certificate.

Scenarios Where a User Might See the Security Alert

- *Scenario A*: The user gets the server certificate for their security appliance from a non-trusted certificate authority; for example, their own certificate authority or cacert.org.

  The user sees the Security Alert pop-up on the first connection attempt but never thereafter until he or she switches to a different security appliance and back.

Recommendation: Administrators should import the root certificate that was used to sign that server certificate (for example, their own certificate authority or cacert.org) into every client machine out of band via E-mail, website, floppy disk, and so on.

- *Scenario B*: The user gets the server certificate for the security appliance from the certificate authority that sits on the security appliance.

  The user sees the Security Alert pop-up on the first connection attempt but never thereafter until he or she switches to a different security appliance and back.

  Recommendation: Administrators should import the root certificate of the certificate authority that sits on the security appliance into every client machine out of band via E-mail, website, floppy disk, and so on.

- *Scenario C*: the security appliance is at default configuration and certificates haven't been configured.

  When at default, the security appliance generates a self-signed server certificate that the AnyConnect client does not trust.

  The user sees the Security Alert pop-up on the first connection attempt but never thereafter until he or she switches to a different security appliance and back.

  Recommendation: Administrators should correctly configure certificates on their security appliance before attempting client connections to them.

In Response to a Microsoft Internet Explorer "Security Alert" Window

The following procedure explains how to install a self-signed certificate as a trusted root certificate on a client in response to a Microsoft Internet Explorer Security Alert window. This window opens when you establish a Microsoft Internet Explorer connection to a security appliance that is not recognized as a trusted site. The upper half of the Security Alert window shows the following text:

```
Information you exchange with this site cannot be viewed or changed by others.
However, there is a problem with the site's security certificate. The security
certificate was issued by a company you have not chosen to trust. View the certificate
to determine whether you want to trust the certifying authority.
```

Install the certificate as a trusted root certificate as follows:

Step 1 Click View Certificate in the Security Alert window.

The Certificate window opens.

Step 2 Click Install Certificate.

The Certificate Import Wizard Welcome opens.

Step 3 Click Next.

The Certificate Import Wizard – Certificate Store window opens.

Step 4 Select "Automatically select the certificate store based on the type of certificate."

Step 5 Click Next.

The Certificate Import Wizard – Completing window opens.

Step 6 Click Finish.

Step 7 Another Security Warning window prompts "Do you want to install this certificate?" Click Yes.

The Certificate Import Wizard window indicates the import is successful.

Step 8 Click OK to close this window.

Step 9 Click OK to close the Certificate window.

Step 10 Click Yes to close the Security Alert window.

The security appliance window opens, signifying the certificate is trusted.

In Response to a Netscape, Mozilla, or Firefox "Certified by an Unknown Authority" Window

The following procedure explains how to install a self-signed certificate as a trusted root certificate on a client in response to a "Web Site Certified by an Unknown Authority" window. This window opens when you establish a Netscape, Mozilla, or Firefox connection to a security appliance that is not recognized as a trusted site. This window shows the following text:

```
Unable to verify the identity of <Hostname_or_IP_address> as a trusted site.
```

Install the certificate as a trusted root certificate as follows:

Step 1 Click the Examine Certificate button in the "Web Site Certified by an Unknown Authority" window.

The Certificate Viewer window opens.

Step 2 Click the "Accept this certificate permanently" option.

Step 3 Click OK.

The security appliance window opens, signifying the certificate is trusted.

Replacing a Digital Certificate with a Trusted Certificate

A trusted Certificate is the most secure option. You can replace the central-site security appliance digital certificate with a trusted certificate by following the procedures in this section. By default, the security appliance has a self-signed Certificate that is regenerated every time the device is rebooted. You can purchase a Certificate from a CA provider like Verisign or Entrust with the name matching the Fully-Qualified Domain Name (FQDN) of your central-site security appliance (for example, vpn.yoursys.com), or you can have the security appliance issue a permanent Certificate for itself by entering the following commands, replacing x.x.x.x with the IP of your security appliance outside or public address:

```
crypto ca trustpoint self
enrollment self
subject-name CN=x.x.x.x,CN=vpn.yoursys.com
crl configure
crypto ca enroll self
ssl trust-point self outside
write
```

When users first connect using AnyConnect, they should click "View Certificate", install this new certificate, then click "Yes" to proceed. The next time they re-connect, they do not see the security alert popup, even if the security appliance is rebooted.

Installing the AnyConnect Client on a User's PC

You can set up a user's PC to run the AnyConnect client in standalone mode by installing the client software for the appropriate operating system directly on the user's PC. In standalone mode, the user starts the AnyConnect client software without first establishing a web connection. The client uses essentially the same authentication mechanisms as the web-enabled (WebLaunch) mode, but the client displays a GUI to the user, asking for the authentication credentials. The following sections describe how to install the client on Windows, Linux, and Mac systems.

- Where to Find the AnyConnect Client Files to Install, page 2-8
- Installing the AnyConnect Client Using the Microsoft Windows Installer on a PC Running Windows, page 2-8
- Installing the AnyConnect Client on a PC Running Linux, page 2-9
- Installing the AnyConnect Client on a PC Running MAC OSX, page 2-9

Where to Find the AnyConnect Client Files to Install

All of the AnyConnect clients are located in the same place.

http://www.cisco.com/cgi-bin/tablebuild.pl/anyconnect

Installing the AnyConnect Client Using the Microsoft Windows Installer on a PC Running Windows

To install the AnyConnect client on a PC running Windows, follow these steps. We suggest you accept the defaults unless your system administrator has instructed otherwise.

Note Vista users must add the security appliance to the trusted zone for automatic installation by the security appliance to work (CSCsh23752).

Step 1 Exit all Windows programs, and disable any antivirus software (recommended).

Step 2 Download the AnyConnect client MSI file from the Cisco site; for example, anyconnect-win-2.0.xxx.msi, where xxx represents the current build number. See the Release Notes for the current release for the full set of operating-system-specific download sites.

Step 3 Double-click the MSI file. The welcome screen for the Cisco AnyConnect VPN Client Setup Wizard displays.

Step 4 Click **Next**. The End-User License Agreement displays. Accept the license agreement and click OK. The Select Installation Folder screen displays.

Step 5 Accept the default folder or enter a new folder and click **Next**. The Ready to Install screen displays.

Step 6 Click **Install**. The client installs and displays the status bar during installation. After installing, the Completing the Cisco AnyConnect VPN Client Setup Wizard screen displays.

Step 7 Click **Next**. The wizard disappears and the installation is complete.

You can also use the Microsoft Installer to load the AnyConnect client software on the user's Windows-based PC. MSI gives Windows users a pre-install package option that provides installation, maintenance, and removal of AnyConnect client software on Windows systems.

Installing the AnyConnect Client on a PC Running Linux

To install the AnyConnect client on a PC Running Linux, follow these steps:

Step 1 For Linux, the client files are contained in a tar/gz file. Unpack the archive with a **tar** command. For example:

```
tar xvzf AnyConnect-Linux-Release-2.0.0xxx.tar.gz
```

The files necessary for installation are placed in the folder *ciscovpn*.

Step 2 Change to the *ciscovpn* folder. As a root user, run the script named *vpn_install.sh*. For example:

```
[root@linuxhost]# cd ciscovpn
[root@linuxhost]# ./vpn_install.sh
```

The client installs in the directory */opt/cisco/vpn*. This script also installs the daemon *vpnagentd* and sets it up as a service that is automatically started when the system boots.

After installing the client, you can start the client manually from the user interface with the Linux command **/opt/cisco/vpn/bin/vpnui** or with the client CLI command **/opt/cisco/vpn/bin/vpn**.

Installing the AnyConnect Client on a PC Running MAC OSX

The AnyConnect client image for MAC OSX is a DMG disk image installation package. To install the AnyConnect client on a system running MAC OSX, follow these steps:

Step 1 Transfer the installation package file to the desktop and double-click the file. Select one of the following files:

- anyconnect-macosx-i386-2.0.xxx.dmg
- anyconnect-macosx-powerpc-2.0.xxx.dmg

This creates a VPN icon representing the installation package file.

Step 2 Double-click the vpn icon to initiate the installation. Follow the sequence of the vpnclient installer, accepting the licensing agreement, selecting the destination volume, and then selecting the "Upgrade" option to perform a basic installation.

Note The installer requires that you authenticate.

The installation is complete.
