CHAPTER 1

Introduction

This guide describes a process for getting the Cisco AnyConnect VPN Client up and running on your central-site security appliance and on your remote users' PCs. In this context, PC refers generically to Windows, Mac, and Linux devices, but the focus in this document is primarily on Windows PC users.

This chapter introduces the Cisco AnyConnect VPN Client and contains the following sections:

AnyConnect Client Features

The Cisco AnyConnect VPN Client is the next-generation VPN client, providing remote users with secure VPN connections to the Cisco 5500 Series Adaptive Security Appliance running ASA version 8.0 and higher or ASDM 6.0 and higher. It does not connect with a PIX device nor with a VPN 3000 Series Concentrator.

Note PIX does not support SSL VPN connections, either clientless or AnyConnect.

The AnyConnect client supports Windows Vista, Windows XP and Windows 2000, Mac OS X (Version 10.4 or later) on either Intel or PowerPC, and Red Hat Linux (Version 9 or later). See the Release Notes for the full set of platform requirements and supported versions.

As the network administrator, you configure the AnyConnect client features on the security appliance. Then, you can load the client on the security appliance and have it automatically download to remote users when they log in, or you can manually install the client as an application on PCs. The client allows user profiles that are displayed in the user interface and define the names and addresses of host computers. The network administrator can assign particular features to individual users or groups.

The AnyConnect client includes the following features. See *Release Notes for Cisco Anyconnect VPN Client, Release 2.3* for the latest information about these features:

- Support for Windows Mobile OS touch-screen devices connecting to Cisco Series 5500 Adaptive Security Appliances. For a list of supported devices, see *Release Notes for Cisco Anyconnect VPN Client, Release 2.3.*

Note Windows Mobile requires a special license and must have ASA Release 8.0.3 or higher running on the security appliance.

- Machine certificate access for authentication (standalone mode only). Any logged-in user on the system in standalone mode can have access to available machine certificates, as well as to user certificates, for VPN authentication.
- The AnyConnect client for Windows Mobile requires that a security appliance mobile license be installed. If the correct license is not installed, end user receives an error message.
- Dynamic Updating of the user interface when changing groups.
- Enhancements to the management of user preferences, including a new profile template and more customizable attributes.
- Enhancements to Application Programming Interface (API), for customers who want to automate a VPN connection with the AnyConnect client from another application, including the following:
  - Preferences
  - Set tunnel-group method

  The API package contains documentation, source files, and library files to support a C++ interface for the Cisco AnyConnect VPN Client. There are libraries and example programs that can be used for building on Windows, Linux and MAC (10.4 or higher) platforms. The Makefiles (or project files) for the Windows platform are also included. For other platforms, there is a platform specific script showing how to compile the example code. Network administrators can link their application (GUI, CLI, or embedded application) with these files and libraries.
- Support for the Component Object Module (COM) technology for Microsoft Windows (not Windows Mobile) environments—COM is a metadata-based protocol that allows programming languages—for example, C++, C#, and Visual Basic—to interact with it. Users can write their own applications in C++, C#, or Visual Basic to interact with the AnyConnect client. These applications can include anything from a new user interface to a simple monitoring/statistical application. Source code for three fully functional sample programs, built with Visual Studio 2005 SP 1 or later, are included with the download in the apiDoc examples directory. The documentation for COM is bundled with the package. See *Release Notes for Cisco Anyconnect VPN Client, Release 2.3* for a summary of the examples included with the COM package.
- Datagram Transport Layer Security (DTLS) with SSL connections—Avoids latency and bandwidth problems associated with some SSL-only 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).
- Standalone Mode—Allows a Cisco AnyConnect VPN client to be established as a PC application without the need to use a web browser to establish a connection.
- Command Line Interface (CLI)—Provides direct access to client commands at the command prompt.
- Microsoft Installer (MSI)—Gives Windows users a pre-install package option that provides installation, maintenance, and removal of AnyConnect client software on Windows systems.
- IPv6 VPN access—Allows access to IPv6 resources over a public IPv4 connection (Windows XP SP2, Windows Vista, Mac OS X, and Linux only).

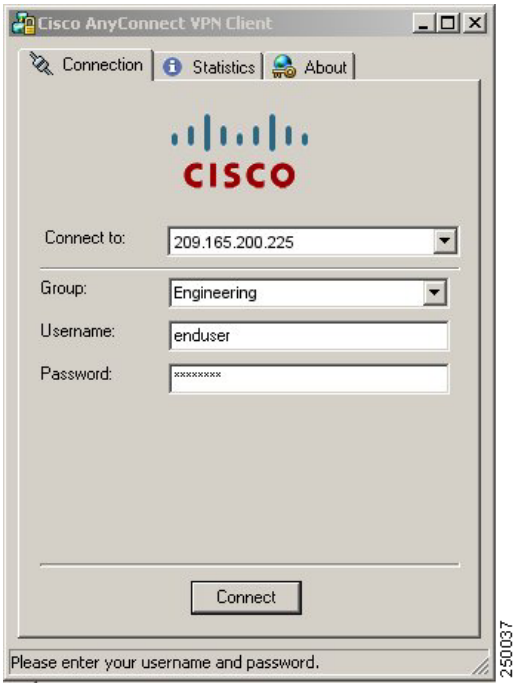
- Start Before Login (SBL)—Allows for login scripts, password caching, drive mapping, and more, for Windows.
- Certificate-only authentication—Allows users to connect with a digital certificate and not provide a user ID and password.
- Simultaneous AnyConnect client and clientless, browser-based connections—Allows a user to have both an AnyConnect (standalone) connection and a Clientless SSL VPN connection (through a browser) at the same time to the same IP address. Each connection has its own tunnel.
- Compression—Increases the communications performance between the security appliance and the client by reducing the size of the packets being transferred. Compression works only for TLS.
- Fallback from DTLS to TLS—Provides a way of falling back from DTLS to TLS if DTLS is no longer working.
- Language Translation (localization)—Provides a way of implementing translation for user messages that appear on the client user interface.
- Dynamic Access Policies feature of the security appliance—Lets you configure authorization that addresses the variables of multiple group membership and endpoint security for VPN connections.
- Cisco Secure Desktop support—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.
- Rekey—Specifies that SSL renegotiation takes place during rekey.
- Support for Start Before Logon for Windows Vista systems, in addition to other Windows operating systems.
- Extended customization and localization features—This version of the AnyConnect client includes enhanced customization features and language translation features. In previous versions, you could customize client installations only on an individual PC basis. With this version, the security appliance can customize the client as it downloads and installs the client on the remote PC. You can also translate the client installer. These extended features include the following items:
  - Localized installs using localized MSI transforms (Windows only).
  - Custom MSI transforms (Windows only).
  - User-defined resource files.
  - Third-party GUI/CLI support.
  - Localization for Mac OS X (10.4 and higher).
- New systray icon—System tray now shows an icon when the AnyConnect client is reconnecting after losing connectivity.
- Application Programming Interface (API)—Lets you create your own GUI and invoke your own programming routines.

Note The Cisco AnyConnect VPN Client can coexist with the IPSec Cisco VPN Client, but they cannot be used simultaneously.

Remote User Interface

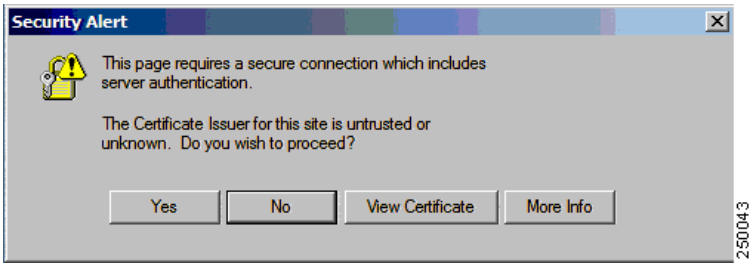
Remote users see the Cisco AnyConnect VPN Client user interface (Figure 1-1). The Connection tab provides a drop-down list of profiles for connecting to remote systems. You can optionally configure a banner message to appear on the Connection tab. The status line at the bottom of the interface shows the status of the connection.

Figure 1-1 Cisco AnyConnect VPN Client User Interface, Connection Tab



If you do not have certificates set up, you might see the dialog box shown in Figure 1-2. When you see this dialog box, click Yes to connect.

Figure 1-2 Security Alert Dialog Box



Note Note: Most users (those with correct certificate deployments) do not see this dialog box.

Table 1-1 shows the circumstances and results when the Security Alert dialog box appears.

Table 1-1 Certificate, Security Alert, and Connection Status

Certificate Status	Does Security Alert Appear?	Client Connection Status
Server certificate sent to the client from the security appliance is independently verifiable *and* the certificate has no serious errors.	No	Success
Server certificate sent to the client from the security appliance is *not* independently verifiable *and* the certificate contains serious errors.	No	Failure
Server certificate sent to the client from the security appliance is *not* independently verifiable *and* the certificate does *not* contain serious errors.	Yes	Because the client cannot verify the certificate, it is still a security concern. The client asks the user whether to continue with the connection attempt.

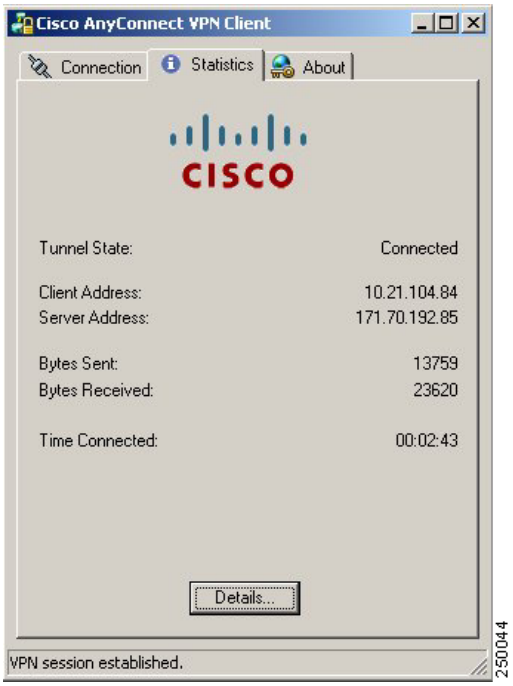
The Security Alert dialog box appears only on the first connection attempt to a given security appliance. After the connection is successfully established, the "thumbprint" of the server certificate is saved in the preferences file, so the user is not prompted on subsequent connections to the same security appliance.

If the user switches to a different security appliance and back, the Security Alert dialog box appears again.

For detailed information and examples of instances in which the remote user does or does not see the Security Alert dialog box, see Configuring and Using User Profiles, page 4-5 and Adding a Security Certificate in Response to Browser Alert Windows, page 2-19.

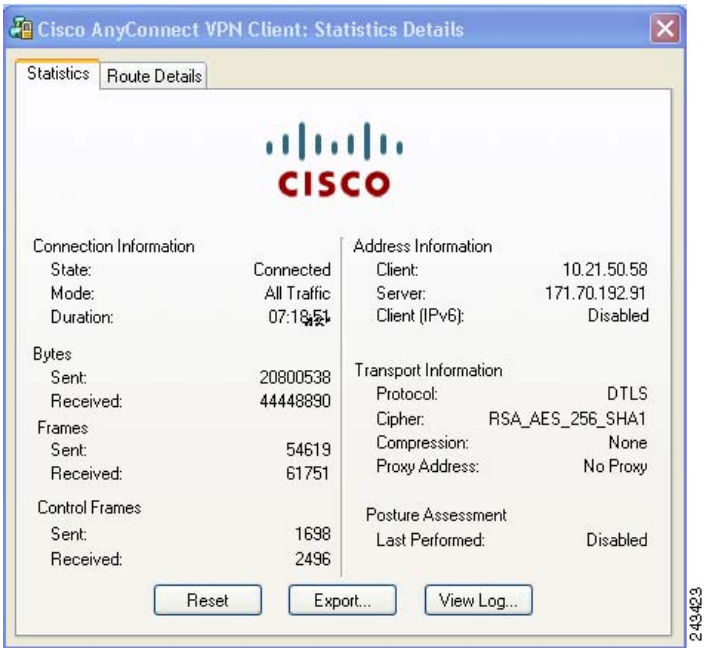
Figure 1-3 shows the Statistics tab, including current connection information.

Figure 1-3 Cisco AnyConnect VPN Client User Interface, Statistics Tab



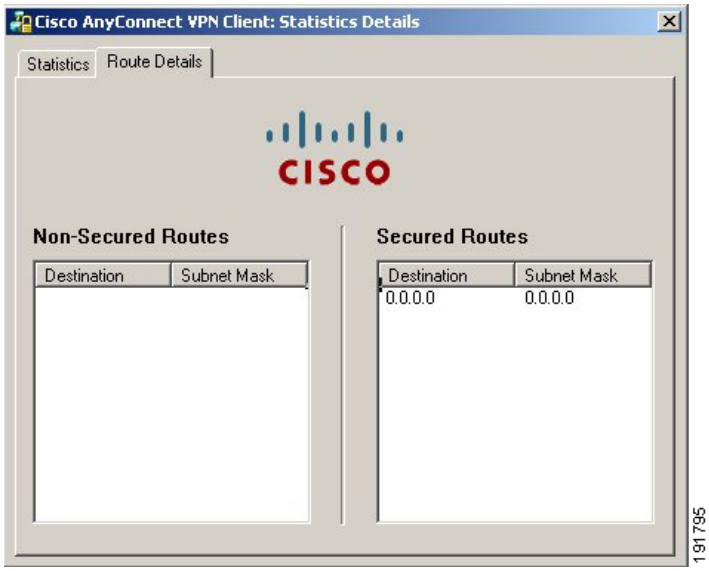
Clicking the Details button opens the Statistics Details window (Figure 1-4). The Statistics tab connection statistics, including the tunnel state and mode, the duration of the connection, the number of bytes and frames sent and received, address information, transport information, and Cisco Secure Desktop posture assessment status. The Reset button on this tab resets the transmission statistics. The Export button lets you export the current statistics, interface, and routing table to a text file. The AnyConnect client prompts you for a name and location for the text file. The default name is AnyConnect-ExportedStats.txt, and the default location is on the desktop.

Figure 1-4 Cisco AnyConnect VPN Client User Interface, Statistics Tab, Statistics Details Tab



Clicking the Route Details tab (Figure 1-5) shows the secured and non-secured routes for this connection. See Viewing Detailed Statistical Information, page 6-4 for information about using the Export and View Log buttons for connection monitoring.

Figure 1-5 Cisco AnyConnect VPN Client User Interface, Statistics Tab, Route Details Tab



Note A Secured Routes entry with the destination 0.0.0.0 and the subnet mask 0.0.0.0 means that all traffic is tunneled.

The About tab (Figure 1-6) shows version, copyright, and documentary information about the Cisco AnyConnect Client.

Figure 1-6 Cisco AnyConnect VPN Client User Interface, About Tab

Getting and Installing the Files You Need

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 is built into the ASA Release 8.0(1) 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.

The latest Release Notes document contains the system requirements and detailed instructions for getting and installing the necessary files. The Windows Vista version of AnyConnect (32- and 64-bit) supports everything that the Windows 2000 and Windows XP versions support, including Start Before Logon. Cisco Secure Desktop, which is a distinct product from AnyConnect, provides 32-bit Vista support for its posture assessment and cache cleaner components. Cisco Secure Desktop does not support secure desktop on Vista at this time.

The client can be loaded on the security appliance and automatically deployed to remote users when they log in to the security appliance, or it can be installed as an application on PCs by a network administrator using standard software deployment mechanisms. You can use a text editor to create user profiles as XML files. These profiles drive the display in the user interface and define the names and addresses of host computers. See Appendix A, “Sample AnyConnect Profile” for a sample AnyConnect user profile.

Where to Find the AnyConnect Client Files

To get the AnyConnect client files and API package, go to http://www.cisco.com/cgi-bin/tablebuild.pl/anyconnect.

Note The API package contains documentation, source files, library files, and binaries to support a C++ interface for the Cisco AnyConnect VPN Client.There are libraries and example binaries for Windows, Linux, and Mac (10.4 or higher) platforms. The Makefiles (or project files) for these platforms are also included. Network administrators can link their application (GUI, CLI, or embedded application) with these files and libraries.

Installing Start Before Logon Components (Windows Only)

The Start Before Logon components must be installed *after* the core client has been installed. Additionally, the AnyConnect 2.2 Start Before Logon components require that version 2.2, or later, of the core AnyConnect client software be installed. If you are pre-deploying the AnyConnect client and the Start Before Logon components using the MSI files (for example, you are at a big company that has its own software deployment—Altiris or Active Directory or SMS.) then you must get the order right. The order of the installation is handled automatically when the administrator loads AnyConnect if it is web deployed and/or web updated.

CSA Interoperability with the AnyConnect Client and Cisco Secure Desktop

If your remote users have Cisco Security Agent (CSA) installed, you must import new CSA policies to the remote users to enable the AnyConnect VPN Client and Cisco Secure Desktop to interoperate with the security appliance.

To do this, follow these steps:

Step 1 Retrieve the CSA policies for the AnyConnect client and Cisco Secure Desktop. You can get the files from:

- The CD shipped with the security appliance.
- The software download page for the ASA 5500 Series Adaptive Security Appliance at http://www.cisco.com/cgi-bin/tablebuild.pl/asa.

The filenames are AnyConnect-CSA.zip and CSD-for-CSA-updates.zip

Step 2 Extract the .export files from the .zip package files.

Step 3 Choose the correct version of the .export file to import. The Version 5.2 export files work for CSA Versions 5.2 and higher. The 5.x export files are for CSA Versions 5.0 and 5.1.

Step 4 Import the file using the Maintenance > Export/Import tab on the CSA Management Center.

Step 5 Attach the new rule module to your VPN policy and generate rules.

For more information, see the CSA document *Using Management Center for Cisco Security Agents 5.2*. Specific information about exporting policies is located in the section *Exporting and Importing Configurations.*