CHAPTER 1

Introduction to the AnyConnect Secure Mobility Client

The Cisco AnyConnect Secure Mobility client is the next-generation VPN client, providing remote users with secure IPsec (IKEv2) or SSL VPN connections to the Cisco 5500 Series Adaptive Security Appliance (ASA). AnyConnect provides end users with a connectivity experience that is intelligent, seamless and always-on, with secure mobility across today's proliferating managed and unmanaged mobile devices.

Deployable from the ASA or from Enterprise Software Deployment Systems

AnyConnect can be deployed to remote users from the ASA or using enterprise software deployment systems. When deployed from the ASA, remote users make an initial SSL connection to the ASA by entering the IP address or DNS name in their browser of an ASA configured to accept clientless SSL VPN connections. The ASA presents a login screen in the browser window, and if the user satisfies the login and authentication, downloads the client that matches the computer operating system. After downloading, the client installs and configures itself and establishes an IPsec (IKEv2) or SSL connection to the ASA.

Customizable and Translatable

You can customize the AnyConnect to display your own corporate image to remote users. You can rebrand AnyConnect by replacing our default GUI components, deploy a transform you create for more extensive rebranding, or deploy your own client GUI that uses the AnyConnect API. You can also translate messages displayed by AnyConnect or the installer program in the language preferred by the remote user.

Easily Configured

Using ASDM, you can easily configure AnyConnect features in the client profile—an XML file that provides basic information about connection setup, as well as advanced features such as Start Before Logon (SBL). For some features, you also need to configure the ASA. The ASA deploys the profile during AnyConnect installation and updates.

Additional Supported Modules

The Cisco AnyConnect Secure Mobility client, Version 3.0, integrates new modules into the AnyConnect client package:

- Network Access Manager—(Formerly called the Cisco Secure Services Client) Provides Layer 2 device management and authentication for access to both wired and wireless networks.

- Posture Assessment—Provides the AnyConnect Secure Mobility Client the ability to identify the operating system, antivirus, antispyware, and firewall software installed on the host prior to creating a remote access connection to the ASA. Based on this prelogin evaluation, you can control which hosts are allowed to create a remote access connection to the security appliance. The Host Scan application is delivered with the posture module and is the application that gathers this information.
- Telemetry—Sends information about the origin of malicious content detected by the antivirus software to the web filtering infrastructure of the Cisco IronPort Web Security Appliance (WSA), which uses this data to provide better URL filtering rules.
- Web Security—Routes HTTP and HTTPS traffic to the ScanSafe Web Security scanning proxy server for content analysis, detection of malware, and administration of acceptable use policies.
- Diagnostic and Reporting Tool (DART)—Captures a snapshot of system logs and other diagnostic information and creates a .zip file on your desktop so you can conveniently send troubleshooting information to Cisco TAC.
- Start Before Logon (SBL)—Starts AnyConnect before the Window dialog box appears and forces the user to connect to the enterprise infrastructure over a VPN connection before logging on to Windows by starting AnyConnect before the Windows login dialog box appears.

This chapter includes the following sections:

AnyConnect License Options

The AnyConnect Secure Mobility client requires license activation to support VPN sessions. We provide three tiers of license options, depending on the AnyConnect client and Secure Mobility features and the number of sessions you want to support:

- AnyConnect Essentials—Supports the AnyConnect Secure Mobility client. This license supports all AnyConnect client features except those labeled as Premium or It also supports sessions established using our legacy client, the Cisco VPN Client. You activate this license on the adaptive security appliance.
- Premium—Supports all AnyConnect Essentials features, browser-based VPN access, the Premium AnyConnect client features, and Cisco Secure Desktop for both browser-based and AnyConnect sessions. You activate this license on the adaptive security appliance.
- AnyConnect Secure Mobility—Supports web security features. You activate this license on the Cisco web security appliance. The license name depends on the license adaptive security appliance:
- A Cisco IronPort Web Security Appliance license .

An adaptive security appliance activated with an AnyConnect Premium license activated on the ASA supports the same access technologies supported by the AnyConnect Essentials license plus the following AnyConnect Secure Mobility client premium features:

- Always-on VPN and associated optional features: closed connect failure policy, captive portal remediation, local printing, and tethered device support.
- Cisco Secure Desktop.
- Optimal Gateway Selection.
- Firewall rules per group policy.
- User message if a VPN session enters a quarantine state.

Both the AnyConnect Essentials and AnyConnect Premium licenses have tiered options that specify the total number of VPN sessions supported.

A Cisco IronPort Web Security Appliance activated with a Cisco Secure Mobility for AnyConnect Premium license or Cisco Secure Mobility for AnyConnect Essentials license lets you provide the following services for browser-based SSL sessions and AnyConnect VPN sessions with adaptive security appliances:

- Enforce acceptable use policies and protect endpoints from websites found to be unsafe by granting or denying all HTTP and HTTPS requests.
- Provide administrator access to Internet usage reports for all VPN sessions.

These services require a Cisco IronPort Web Security Appliance license. A Cisco Secure Mobility for AnyConnect Premium license activation also requires activation of either an AnyConnect Premium or an AnyConnect Essentials license on the adaptive security appliance. A Cisco Secure Mobility for AnyConnect Essentials license activation also requires activation of an AnyConnect Essentials license on the adaptive security appliance. You cannot use an essentials license activated on a web security appliance in combination with a Premium license activated on an adaptive security appliance. The AnyConnect license activated on the web security appliance must match or exceed the number of VPN sessions supported by the AnyConnect license activated on the adaptive security appliance.

Standalone and WebLaunch Options

The user can use AnyConnect in the following modes:

- Standalone mode—Lets the user establish an AnyConnect connection without using a web browser. If you have permanently installed AnyConnect on the user's PC, the user can run in standalone mode. In standalone mode, a user opens AnyConnect just like any other application and enters the username and password credentials into the fields of the AnyConnect GUI. Depending on how you configure the system, the user might also be required to select a group. When the connection is established, the ASA checks the version of AnyConnect on the user's PC and, if necessary, the client downloads the latest version.
- WebLaunch mode—Lets the user enter the URL of the ASA in the Address or Location field of a browser using the HTTPS protocol. The user then enters the username and password information on a Logon screen, selects the group, and clicks **Submit**. If you have specified a banner, that information appears, and the user acknowledges the banner by clicking **Continue**.

  The portal window appears. To start AnyConnect, the user clicks **Start AnyConnect** on the main pane. A series of documentary windows appears. When the Connection Established dialog box appears, the connection is working, and the user can proceed with online activities.

If you configure the ASA to deploy the AnyConnect package, you ensure that the ASA is the single point of enforcement as to which versions of AnyConnect can establish a session, even if you deploy AnyConnect with an enterprise software deployment system. When you load an AnyConnect package on the ASA, you enforce a policy to which only versions as new as the one loaded on the ASA can connect. AnyConnect upgrades itself when it connects to the ASA. Alternatively, you can deploy a local

policy file that specifies whether the client bypasses the client downloader, eliminating the requirement for the client package file on the ASA. However, other features such as weblaunch and automatic updates are disabled.

AnyConnect Licensing Options

The following sections associate the licensing options with the AnyConnect components.

Network Access Manager

The AnyConnect Network Access Manager is licensed without charge for use with Cisco wireless access points, wireless LAN controllers, switches, and RADIUS servers. No AnyConnect Essentials or Premium license is required. A current SmartNet contract is required on the related Cisco equipment.

Web Security

Web security requires a Web Security license that specifies the number of supported endpoints.

VPN Licensing

AnyConnect support for SSL and IKEv2 access requires either of the following licenses to specify the maximum number of remote access sessions supported at a time:

- AnyConnect Essentials license.
- AnyConnect Premium SSL VPN Edition license.

Either license supports the basic AnyConnect features.

Table 1-1 shows the licenses you can combine with the Essentials and Premium licenses.

Table 1-1 Advanced AnyConnect License Options for VPN

Sessions License	License Option	Basic Access	Post Log-in Always-on VPN	Malware Defense, Acceptable Use Policy Enforcement, and Data Leakage Prevention on the Web	Clientless Access	Endpoint Assessment	Endpoint Remediation	Business Continuity
AnyConnect Essentials	(base license)	✓						
	Cisco Secure Mobility for AnyConnect Essentials	✓	✓	✓				
AnyConnect Premium SSL VPN Edition	(base license)	✓	✓		✓	✓		
	Cisco Secure Mobility for AnyConnect Premium	✓	✓	✓	✓	✓		
	Advanced Endpoint Assessment	✓	✓		✓	✓	✓	
	Flex[1]	✓	✓	✓	✓	✓	✓	✓

1. A flex license provides business continuity support for malware defense, acceptable use policy enforcement, data leakage prevention on the web, and endpoint remediation features only if those features are licensed.

The *AnyConnect Essentials*, *AnyConnect Premium SSL VPN Edition*, *Advanced Endpoint Assessment*, and *Flex* licenses require activation on a Cisco adaptive security appliance (ASA) running 8.0(x) or later; however, some features require later versions of the ASA.

The *Cisco Secure Mobility* licenses requires activation on a Cisco IronPort Web Security Appliance (WSA) running 7.0 or later.

The activation of an *AnyConnect Mobile* license on the ASA supports mobile access but does not provide support for the features in this table. It is available as an option with either an AnyConnect Essentials or an AnyConnect Premium SSL VPN Edition license.

For a list of the features available with either an AnyConnect Essentials license or AnyConnect Premium SSL VPN Edition license, see the Basic Features table.

The features enabled by the optional licenses shown in Table 1-1 are as follows:

- *Post Log-in Always-on VPN* establishes a VPN session automatically after the user logs in to a computer. For more information, see Always-on VPN. This feature also includes a Connect Failure Policy for Always-on VPN and Captive Portal Hotspot Detection and Remediation.

- *Malware defense, acceptable use policy enforcement and data leakage prevention for the web* are features provided by the Cisco IronPort Web Security Appliance (WSA). For more information, see the *Cisco IronPort Web Security Appliances Introduction*.
- *Clientless access* lets you use a browser to establish a VPN session and lets specific applications use the browser to access that session.
- *Endpoint assessment* ensures that your choice of antivirus software versions, antispyware versions, associated update definitions, firewall software versions, and corporate property verification checks comply with policies to qualify a session to be granted access to the VPN.
- *Endpoint remediation* attempts to resolve endpoint failures to satisfy corporate requirements for antivirus, antispyware, firewall software, and definitions file requirements.
- *Business continuity* increases the number of licensed remote access VPN sessions to prepare for temporary spikes in usage during cataclysmic events such as pandemics. Each flex license is ASA-specific and provides support for sixty days. The count can consist of both contiguous and noncontiguous days.

Cisco Secure Remote Access: VPN Licensing Overview provides brief descriptions of the AnyConnect license options and example SKUs.

For a detailed list of the AnyConnect features, license and release requirements, and the endpoint OSs supported for each feature, see *Cisco End User License Agreement, AnyConnect Secure Mobility Client, Release 3.0*.

Configuration and Deployment Overview

Use the AnyConnect Profile editor to configure the AnyConnect features in the profile file; then configure the ASA to download this file along with AnyConnect client automatically when users make a VPN connection to the ASA with a browser. The profile file drives the display in the user interface and defines the names and addresses of host computers. By creating and assigning different profiles to group policies configured on the ASA, you can differentiate access to these features. Following assignment to the respective group policies, the ASA automatically pushes the profile assigned to the user upon connection setup.

Profiles provide basic information about connection setup, and users cannot manage or modify them. The profile is an XML file that lets you identify the secure gateway (ASA) hosts that you want to make accessible. In addition, the profile conveys additional connection attributes and constraints on a user. For some features, you can specify some settings in the profile as user controllable. The AnyConnect GUI displays controls for these settings to the end user.

Usually, a user has a single profile file. This profile contains all the hosts needed by a user, and additional settings as needed. In some cases, you might want to provide more than one profile for a given user. For example, someone who works from multiple locations might need more than one profile. Be aware, however, that some of the profile settings, such as Start Before Login, control the connection experience at a global level. Other settings, such as those unique to a particular host, depend on the host selected.

Alternatively, you can use an enterprise software deployment system to install the profile file and client as an application on computers for later access.

AnyConnect Secure Mobility Feature Configuration Guidelines

AnyConnect Secure Mobility is a set of features you can configure to optimize the security of the VPN endpoints. To configure all of the AnyConnect secure mobility client options, refer to the following sections:

Step 1 Go to the "Configuring the ASA for WSA Support of the AnyConnect Secure Mobility Solution" section on page 2-46.

Step 2 Use the *Cisco AnyConnect Secure Mobility Solution Guide* as a guide to configuring a WSA to support AnyConnect.

Step 3 Use the AnyConnect Profile Editor to configure the following features:

- Trusted Network Detection, page 3-17
- Always-on VPN, page 3-19
- Disconnect Button for Always-on VPN, page 3-25
- Connect Failure Policy for Always-on VPN, page 3-26
- Captive Portal Hotspot Detection and Remediation, page 3-29
- Certificate Enrollment using SCEP, page 3-34

API

Use the Application Programming Interface (API) if you want to automate a VPN connection with AnyConnect 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 AnyConnect. You can use libraries and example programs for building AnyConnect on Windows, Linux, and Mac OS X. The API package includes project files (Makefiles) for the Windows platform. For other platforms, a platform-specific script shows how to compile the example code. You can link your application (GUI, CLI, or embedded application) with these files and libraries.

The API supports only the VPN functionality of the client. It does not support the optional AnyConnect modules, such as the Network Access Manager, Web Security, and telemetry.

Installing Host Scan

To reduce the chances of intranet infection by hosts establishing VPN connections, you can configure Host Scan to download and check for antivirus, antispyware, and firewall software (and associated definitions file updates as a condition for the establishment of a VPN session). Host Scan was once only available as a component of Cisco Secure Desktop (CSD). In this release of AnyConnect Secure Mobility Client, host scan is now a separate module that you can install and update separately from CSD.

Note Host Scan and some third-party firewalls can interfere with the firewall function optionally deployed by the group policy.

See Chapter 5, "Configuring Host Scan" for more information about installing and managing host scan.