About This Guide

OL-12950-012

This preface introduces the *Cisco AnyConnect VPN Client Administrator Guide*, and includes the following sections:

Document Objectives

The purpose of this guide is to help you configure the Cisco AnyConnect VPN Client parameters on the security appliance. This guide does not cover every feature, but describes only the most common configuration scenarios.

You can configure and monitor the security appliance by using either the command-line interface or ASDM, a web-based GUI application. ASDM includes configuration wizards to guide you through some common configuration scenarios, and online Help for less common scenarios. For more information, see: http://www.cisco.com/univercd/cc/td/doc/product/netsec/secmgmt/asdm/index.htm

This guide applies to the Cisco ASA 5500 series security appliances (ASA 5505 and higher). Throughout this guide, the term “security appliance” applies generically to all supported models, unless specified otherwise. The PIX family of security appliances is not supported.

Audience

This guide is for network managers who perform any of the following tasks:

- Manage network security
- Install and configuresecurity appliances
- Configure VPNs

Related Documentation

For more information, refer to the following documentation:

- *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*
- *Cisco ASA 5500 Series Release Notes*
- *Cisco ASDM Release Notes*
- *Cisco ASDM Online Help*
- *Release Notes for Cisco AnyConnect VPN Client, Release 2.0*
- *Cisco Security Appliance Command Reference*
- *Cisco Security Appliance Logging Configuration and System Log Messages*
- *Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*
- For Open Source License information for this product, please see the following link: http://www.cisco.com/en/US/docs/security/asa/asa80/license/opensrce.html#wp50053.

Document Organization

This guide includes the chapters and appendixes described in Table 1.

Table 1 Document Organization

Chapter/Appendix	Definition
Chapter 1, "Introduction"	Provides a high-level overview of the Cisco Anyconnect VPN Client.
Chapter 2, "Common AnyConnect VPN Client Installation and Configuration Procedures"	Describes how to access the required files and install the Cisco AnyConnect VPN Client on the security appliance and on the remote user PCs.
Chapter 3, "Installing the AnyConnect Client and Configuring the Security Appliance with ASDM"	Describes how to use ASDM to install the Cisco AnyConnect VPN Client on the security appliance.
Chapter 4, "Installing the AnyConnect Client on a Security Appliance Using CLI"	Describes how to use the command-line interface to install the Cisco AnyConnect VPN Client on the security appliance.
Chapter 5, "Configuring AnyConnect Features Using ASDM"	Describes how to use ASDM to configure the various features of the Cisco AnyConnect VPN Client on the security appliance.
Chapter 6, "Configuring AnyConnect Features Using CLI"	Describes how to use ASDM to configure the various features of the Cisco AnyConnect VPN Client on the security appliance.
Chapter 7, "Configuring and Using AnyConnect Client Operating Modes and User Profiles"	Describes how to configure and use AnyConnect client operating modes and XML users profiles.

Table 1 Document Organization (continued)

Chapter/Appendix	Definition
Chapter 8, "Customizing and Localizing the AnyConnect Client"	Describes how to customize and localize the end-user interface of the Cisco AnyConnect VPN Client.
Chapter 9, "Monitoring and Maintaining the AnyConnect Client"	Describes how to monitor and maintain the Cisco AnyConnect VPN Client using the security appliance
Appendix A, "Sample AnyConnect Profile and XML Schema"	Provides a sample AnyConnect user XML profile and an XML schema that you can use to validate the user profiles you create.
Appendix B, "Using Microsoft Active Directory to Add the Security Appliance to the List of Internet Explorer Trusted Sites for Domain Users"	Describes in detail how an Active Directory Domain Administrator can push to remote users a group policy that adds the security appliance to the list of trusted sites in Internet Explorer.

Document Conventions

Command descriptions use these conventions:

- Braces ({ }) indicate a required choice.
- Square brackets ([ ]) indicate optional elements.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Right-pointing angle brackets (>) indicate a sequence in a path.
- **Boldface** indicates commands and keywords that are entered literally as shown.
- *Italics* indicate arguments for which you supply values.

Examples use these conventions:

- Examples depict screen displays and the command line in `screen` font.
- Information you need to enter in examples is shown in **`boldface screen`** font.
- Variables for which you must supply a value are shown in *`italic screen`* font.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Licensing

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).