cisco.



Cisco VPN Client Administrator Guide

Release 5.0 April 2010

Americas Headquarters Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134-1706 USA

http://www.cisco.com Tel: 408 526-4000

800 553-NETS (6387)

Fax: 408 527-0883

Text Part Number: OL-5492-02

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Cisco VPN Client Administrator Guide Copyright © 2008 Cisco Systems, Inc. All rights reserved.



About This Guide

This *VPN Client Administrator Guide* tells you how to set up selected features of the Cisco VPN Client for users. This manual supplements the information provided in accompanying documentation for the Cisco VPN devices that work with the VPN Client. The chapters and sections in this manual apply to all platforms supported by the Cisco VPN Client unless otherwise specified.

The VPN Client is an IPsec software client that lets users:

- Connect to a Cisco VPN device
- · Capture, filter, and display messages generated by the VPN Client software
- Enroll for and manage certificates
- Manually change the size of the maximum transmission unit (see Changing the MTU Size)

For information about how to use this application, see the VPN Client User Guide for your platform.

In this administrator guide, the term Cisco VPN device refers to the following Cisco products:

- Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco VPN 3000 Series Concentrator
- Cisco Secure PIX Firewall devices
- IOS platform devices, such as the Cisco xxxx Series Routers

Audience

We assume you are an experienced system administrator or network administrator with appropriate education and training, who knows how to install, configure, and manage internetworking systems. You should be familiar with system configuration and management for the platform you are administering.

OL-5492-02

Organization

xii

The VPN Administrator Guide is organized as follows:

Chapter	Title	Description	
Chapter 1	Configuration Information for an Administrator	Provides administration information common across all platforms.	
Chapter 2	Configuring the VPN Client Using ASDM	Explains how to use ASDM to configure A Cisco Series 5500 Adaptive Security Appliance for VPN Client connections.	
Chapter 3	Configuring VPN Client Parameters Using CLI	Explains how to use the ASA command-line interface to configure A Cisco Series 5500 Adaptive Security Appliance for VPN Client connections.	
Chapter 4	Configuring the VPN Client on a VPN 3000 Series Concentrator	Explains how to configure a VPN 3000 Concentrator for remote access, personal firewalls, local LAN access, backup servers, NAT-T. Also describes how to configure a VPN Client to work with Entrust Entelligence and smart cards.	
Chapter 5	Preconfiguring the VPN Client for Remote Users	Shows how to create global and user profiles.	
Chapter 6	Updating VPN Client Software on a VPN 3000 Concentrator	Describes how to update VPN Client software manually and automatically for all VPN Client platforms.	
Chapter 7	Configuring Automatic VPN Initiation—Windows Only	Describes auto initiation and how to configure the vpnclient.ini file for auto initiation.	
Chapter 8	Using the VPN Client Command-Line Interface	Explains how to use the command-line interface (CLI) to connect to a VPN device, how to disconnect from a VPN device, and how to get status information from a VPN device. You can use these commands in batch mode.	
Chapter 9	Managing Digital Certificates from the Command Line	Explains how to use the command-line interface (CLI) to manage digital certificates.	
Chapter 10	Customizing the VPN Client Software	Describes how to use your own names and icons for the VPN Client applications instead of Cisco Systems names. Also describes how to install and reboot the VPN Client software without user interaction, called <i>silent mode</i> .	

Chapter	Title	Description
Chapter 11	Troubleshooting and Programmer Notes	Lists troubleshooting techniques. Describes how to use the SetMTU application.
Chapter 12	Windows Installer (MSI) Information	Describes alternative ways to start MSI, explains logging and upgrading.

Related Documentation

For the complete list of Cisco VPN Client documentation, see: http://www.cisco.com/en/US/products/sw/secursw/ps2308/tsd_products_support_series_home.html. The VPN Client Administrator Guide is being updated at this time.

This administrator guide is a companion to the following VPN Client user guides:

- VPN Client User Guide for Windows, Release 5.0— explains to Windows VPN Client users how to
 install the VPN Client for Windows software, configure connection entries, connect to Cisco VPN
 devices, manage VPN connections, and enroll for digital certificates.
- VPN Client User Guide for Mac OS X, Release 4.6— explains to Mac VPN Client users how to install the VPN Client for Mac software, configure connection entries, connect to Cisco VPN devices, manage VPN connections, and enroll for digital certificates. The VPN Client on the Macintosh platform can be managed through the GUI or the command-line interface.
- VPN Client User Guide for Linux and Solaris, Release 4.6— explains to Linux and Solaris VPN Client users how to install the VPN Client software, configure connection entries, connect to Cisco VPN devices, manage VPN connections, and enroll for digital certificates. The VPN Client on the Linux and Solaris platforms is managed only through the command-line interface.
- Also the VPN Client includes an online HTML-based help system that you can access through a
 browser in several ways: clicking the Help icon on the Cisco Systems VPN Client programs menu
 (Start>Programs>Cisco Systems VPN Client>Help), pressing F1 while using the applications, or
 clicking the Help button on screens that include it.
- Release Notes for the Cisco VPN Client Version 5.0.x—includes information relevant to all platforms.

To view the latest version of the VPN Client documentation on the Cisco Web site, see: http://www.cisco.com/en/US/products/sw/secursw/ps2308/tsd products support series home.html

Cisco ASA 5500 Series Adaptive Security Appliance Documentation

For the complete list of Cisco ASA 5500 Series Adaptive Security Appliance documentation, see: http://www.cisco.com/en/US/docs/security/asa/roadmap/asaroadmap.html. In each instance, be sure to check the www.cisco.com documentation website for the specific software and documentation version that you are using.

ASA Version 8.0 Documentation Set



See also the "Cisco ASDM Documentation" section.

Getting Started (5500)—*Cisco ASA 5500 Getting Started Guide, Software Version 8.0* http://www.cisco.com/en/US/docs/security/asa/asa80/getting_started/asa5500/quick/guide/5500gsg.ht ml

Getting Started (5505)—Cisco ASA 5505 Getting Started Guide, 8.0 http://www.cisco.com/en/US/docs/security/asa/asa80/getting_started/asa5505/quick/guide/5505gsg.html

GUI Configuration—ASDM 6.0 User Guide

http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/user/guide/usrguide.html

Selected ASDM Configuration Topics—These documents explain how to use ASDM to configure selected VPN features.

- Clientless SSL VPN Login Screen Advanced Customization
 http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/selected_topics/adv_custom.html
- Displaying Multiple Languages to SSL VPN Users
 http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/selected_topics/disp_2lang.html

CLI Configuration—*Cisco Security Appliance Command Line Configuration Guide, Version 8.0* http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/conf gd.html

Command Reference—Cisco Security Appliance Command Reference, Version 8.0 http://www.cisco.com/en/US/docs/security/asa/asa80/command/reference/cmd_ref.html

Syslog Messages—*Cisco Security Appliance System Log Messages, Version* 8.0 http://www.cisco.com/en/US/docs/security/asa/asa80/system/message/syslog.html

ASA 8.0 Release Notes—Release notes for each maintenance release: http://www.cisco.com/en/US/products/ps6120/prod_release_notes_list.html

ASDM 6.0 Release Notes—Release notes for each maintenance release: http://www.cisco.com/en/US/products/ps6121/prod release notes list.htm

Open Source Software Licenses for ASA and PIX Security Appliances, Version 8.0 http://www.cisco.com/en/US/docs/security/asa/asa80/license/opensrce.html

Cisco ASDM Documentation

ASDM is the graphical user interface for the Cisco ASA 5500 Series Adaptive Security Appliance.



The documentation for a given ASDM version includes the feature set for the latest ASA platform version. For example, ASDM Version 6.1 supports ASA Version 8.0 and Version 8.1, so the ASDM guide includes all of the features for ASA Version 8.1. ASA Version 8.0 users do not have a separate guide that includes only Version 8.0 platform features.

ASDM 6.1 Documentation Set

Configuration—Cisco ASDM User Guide, 6.1

http://www.cisco.com/en/US/docs/security/asdm/6 1/user/guide/usergd.html

Release Notes—Release notes for each maintenance release:

http://www.cisco.com/en/US/products/ps6121/prod release notes list.html

VPN 3000 Series Concentrator Documentation

For the complete list of VPN 3000 Series Concentrator documentation, see: http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/tsd_products_support_eol_series_home.ht ml



This product is no longer being sold. For additional information, view the End-of-Sale/End-of-Life Notice at

 $http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5743/ps5749/ps2284/prod_end-of-life_notice0\\900aecd805cd5a0.html$

The VPN 3000 Concentrator Getting Started, Release 4.1 guide explains how to unpack and install the VPN 3000 Concentrator, and how to configure the minimal parameters. This is known as Quick Config.

The VPN 3000 Concentrator Reference Volume I: Configuration, Release 4.1 explains how to start and use the VPN 3000 Concentrator Manager. It details the Configuration screens and explains how to configure your device beyond the minimal parameters you set during quick configuration.

The VPN 3000 Concentrator Reference Volume II: Administration and Monitoring, Release 4.1 provides guidelines for administering and monitoring the VPN 3000 Concentrator. It explains and defines all functions available in the Administration and Monitoring screens of the VPN 3000 Concentrator Manager. Appendixes to this manual provide troubleshooting guidance and explain how to access and use the alternate command-line interface.

The VPN 3000 Concentrator Manager (the Manager) also includes online help that you can access by clicking the **Help** icon on the toolbar in the Manager window.

IOS Documentation

You can find the IOS documentation set at the following URL:

http://www.cisco.com/en/US/products/ps6350/tsd_products_support_series_home.html

Other References

Other useful references include:

- Virtual Private Networking: An Overview. Microsoft Corporation. (Available from Microsoft website.)
- www.ietf.org for Internet Engineering Task Force (IETF) Working Group drafts on IP Security Protocol (IPsec).
- www.whatis.com, a web reference site with definitions for computer, networking, and data communication terms.

Conventions

This document uses the following conventions:

Convention	Description
boldface font	User actions and commands are in boldface .
italic font	Arguments for which you supply values are in <i>italics</i> .
screen font	Terminal sessions and information the system displays are in screen font.
boldface screen font	Information you must enter is in boldface screen font in the command-line interface (for example, vpnclient stat).
italic screen font	Arguments for which you supply values are in <i>italic</i> screen font.

Notes use the following conventions:



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

Cautions use the following conventions:



Means *reader be careful*. Cautions alert you to actions or conditions that could result in equipment damage or loss of data.

Data Formats

As you configure and manage the system, enter data in the following formats unless the instructions indicate otherwise:

Type of Data	Format
IP Addresses	IP addresses use 4-byte dotted decimal notation (for example, 192.168.12.34); as the example indicates, you can omit leading zeros in a byte position.
Subnet Masks and Wildcard Masks	Subnet masks use 4-byte dotted decimal notation (for example, 255.255.255.0). Wildcard masks use the same notation (for example, 0.0.0.255); as the example illustrates, you can omit leading zeros in a byte position.
MAC Addresses	MAC addresses use 6-byte hexadecimal notation (for example, 00.10.5A.1F.4F.07).
Hostnames	Hostnames use legitimate network hostname or end-system name notation (for example, VPNO1). Spaces are not allowed. A hostname must uniquely identify a specific system on a network.
Text Strings	Text strings use upper- and lower-case alphanumeric characters. Most text strings are case-sensitive (for example, simon and Simon represent different usernames). In most cases, the maximum length of text strings is 48 characters.
Port Numbers	Port numbers use decimal numbers from 0 to 65535. No commas or spaces are permitted in a number.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, 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

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) Website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- · Resolve technical issues with online support
- Download and test software packages
- · Order Cisco learning materials and merchandise
- · Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The avenue of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Cisco TAC Website

You can use the Cisco TAC website to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://tools.cisco.com/RPF/register/register.do

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

http://www.cisco.com/en/US/support/index.html

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC website so that you can describe the situation in your own words and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

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).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- 1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
- 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
- 3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)".
- 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
- 5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
- 6. Redistributions of any form whatsoever must retain the following acknowledgment:
 "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)".

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- 1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
- 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- 3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
 - "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".
 - The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
- 4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Notices



CHAPTER

Configuration Information for an Administrator

This chapter provides information to a network administrator that supplements the VPN Client User Guide for your platform and the configuration guide for the secure gateway that you are using, either a Cisco Series 5500 Adaptive Security Appliance or a Cisco VPN 3000 Series Concentrator. While this chapter sometimes, for completeness, mentions IPsec site-to-site connections, this document is concerned only with IPsec remote-access connections.

This chapter includes the following major topics:

- IPsec Concepts, page 1-1
- System Requirements, page 1-3
- Using the VPN Client, page 1-5
- Advisories for Windows Vista Users, page 1-6
- API for Cisco VPN Client, page 1-6
- Configuring the VPN Client, page 1-7
- Configuring Entrust Entelligence for the VPN Client—Windows Only, page 1-10
- Setting up the VPN Client for Authentication using Smart Cards—Windows Only, page 1-12
- Configuring Mutual Group Authentication, page 1-13
- Configuring IKE Parameters, page 1-13
- Configuring VPN Client Firewall Policy for Windows, page 1-17
- Overview of Client Firewalls, page 1-17
- Configuring the VPN Client on a Central-site Device, page 1-22

IPsec Concepts

IPsec provides the most complete architecture for VPN tunnels, and it is often perceived as the most secure protocol. Both LAN-to-LAN (site-to-site) connections and client-to-LAN connections can use IPsec.

In IPsec terminology, a "peer" is a remote-access client or another secure gateway. During tunnel establishment with IPsec, the two peers negotiate security associations that govern authentication, encryption, encapsulation, and key management. These negotiations involve two phases: first, to establish the tunnel (the IKE SA); and second, to govern traffic within the tunnel (the IPsec SA).

In IPsec site-to-site connections, the security appliance can function as initiator or responder. In IPsec remote-access (client-to-LAN) connections, the security appliance functions only as responder. Initiators propose SAs; responders accept, reject, or make counter-proposals—all in accordance with configured SA parameters. To establish a connection, both entities must agree on the SAs.

The VPN Client complies with the IPsec protocol and is specifically designed to work with the security appliance. However, the security appliance can establish IPsec connections with many protocol-compliant clients. Likewise, the security appliance can establish site-to-site connections with other protocol-compliant VPN devices, often called secure gateways.

Supported IPsec Attributes

The security appliance supports these IPsec attributes:

- Main mode for negotiating phase one ISAKMP security associations when using digital certificates for authentication
- Aggressive mode for negotiating phase one ISAKMP Security Associations (SAs) when using preshared keys for authentication
- Authentication Algorithms:
 - ESP-MD5-HMAC-128
 - ESP-SHA1-HMAC-160
- Authentication Modes:
 - Preshared Keys
 - X.509 Digital Certificates
- Diffie-Hellman Groups 1, 2, 5, and 7
- Encryption Algorithms:
 - AES-128, -192, and -256
 - 3DES-168
 - DES-56
 - ESP-NULL
- Extended Authentication (XAuth)
- Mode Configuration (also known as ISAKMP Configuration Method)
- · Tunnel Encapsulation Mode
- IP compression (IPCOMP) using LZS



Smart Card authentication is supported in VPN Client Release 5.0.3.0560 and higher.

Unsupported IPsec Attributes

Cisco VPN Client for Windows Vista, release 5.x, does *not* support the following features:

System upgraded from Windows XP or earlier Windows operating systems to Vista. (Clean OS installation required.)

- Integrated firewall
- · InstallShield.
- · Auto Update.
- Translated Online Help. Online Help is provided only in English.



Start Before Logon is supported only on Windows Vista, Windows XP.

System Requirements

To install the VPN Client on any system, you need

- CD-ROM drive (if you are installing from CD-ROM)
- Administrator privileges

The VPN Client supports the following Cisco VPN devices, referred to in this manual as a secure gateway or a central-site device:

- Cisco ASA 5500 Series Adaptive Security Appliance, all versions
- Cisco VPN 3000 Concentrator Series, Version 3.0 and later.
- Cisco PIX Firewall, Version 6.2.2(122) or Version 6.3(1).
- Cisco IOS Routers, Version 12.2(8)T and later

If you are using Internet Explorer, use version 5.0, Service Pack 2 or higher.

Limitations

The following limitation apply to the VPN Client:

- The VPN Client does not support computers with more than one ethernet or PPP adapter.
- Bluetooth modems used as the Internet media might or might not work with the VPN Client, but they are not officially tested or supported.
- You cannot use the VPN Client and the AnyConnect VPN Client simultaneously on the same system.

Table 1-1 indicates the system requirements to install the VPN Client on each of the supported platforms. For the latest information, refer to the most recent version of the Release Notes for the Cisco VPN Client.

Table 1-1 System Requirements

Computer	Operating System	Requirements
Computer with a Pentium®-class processor or greater, including Tablet PC¹	 Windows 7 32/64-bit Windows Vista 32/64-bit Windows XP 32-bit² 	 Microsoft TCP/IP installed. (Confirm via Start > Settings > Control Panel > Network > Protocols or Configuration.) 50 MB hard disk space.
		RAM: 128 MB for Windows XP (256 MB recommended)
Computer with and Intel x86 processor	RedHat Version 6.2 or later Linux (Intel), or compatible libraries with glibc Version 2.1.1-6 or later, using kernel Versions 2.2.12 or later ³	 32 MB Ram 50 MB hard disk space
	Note The VPN Client does not support SMP (multiprocessor) or 64-bit processor kernels.	
Sun UltraSPARC computer	32-bit or 64-bit Solaris kernel OS Version 2.6 or later	 32 MB Ram 50 MB hard disk space
Macintosh computer	Mac OS X, Version 10.4.0 or later	50 MB hard disk spacePPC or Intel processor.

^{1.} The VPN Client includes support for dual-processor and dual-core workstations for Windows XP and Windows Vista.

Rebootless Client Upgrade for MSI Installer

The MSI installer for the VPN Client installation allows the VPN Client to be upgraded without rebooting under the following circumstances:

- If a previous MSI version of the VPN Client has been installed, overwriting with the 4.8.00.0440 MSI VPN Client installation requires a reboot only to uninstall the previous VPN Client installation. (Prior installations had required an additional reboot that is no longer required.)
- A new installation of the 4.8.00.0440 MSI VPN Client installation does require a reboot.
- Upgrades from the 4.8.00.0440 MSI VPN Client with later MSI installations do *not* require any reboots (CSCsb35946).
- Upgrades from the VPN Client Release 5.x to later versions do not require a reboot.

To enhance the ease of installation of the VPN Client on Windows, the MSI installer launches itself after you unzip the files (CSCeg81066).

The Windows VPN Client Release 4.8.00.440 was the final version that officially supported the Windows 98 operating system. The Windows VPN Client Release 4.6.04.0043 was the final version that officially supported the Windows NT operating system.

Installation of the Linux unified VPN Client works correctly during the kernel module build with Linux kernel 2.2.19 and later (CSCsg98579)



In certain uncommon instances, MSI reboot might be required, depending on the results from the DNE installer.

MSI Installation with the Japanese Language Help Files

The Japanese help files for the MSI transform have been removed from the VPN Client installation package. They are now posted separately on www.cisco.com as "vpnclient_help_jp_4.8.00.0440.zip" (CSCei23559).

Bypassing Installation of Firewall Files When Stateful Firewall Is Not Required

In some cases, the Stateful Firewall files of the VPN Client conflict with other third party applications. To minimize this conflict, you can install the VPN Client without its Stateful Firewall files by using the following procedures:



Do not use this procedure if you are using a Zone Alarm product, because they share similar files.

If the workstation does *not* have the vsdata.dll file (no former Cisco VPN Client installation or Zone Alarm products), then delete or rename this file before proceeding.

MSI must use the novsdata.zip transform posted on www.cisco.com for VPN Client versions prior to Release 5.x. The transform is incompatible with the 5.x releases. Beginning with VPN Client Release 5.0.3.0560, an MSI installation flag was added to avoid the installation of the guild in firewall files (CSCsi45962):

msiexec.exe /i vpnclient_setup.msi DONTINSTALLFIREWALL=1

This prevents the VPN Client from installing or updating the following files:

vsdata.dll

vsinit.dll

vsdatant.sys

Manually removing or renaming these files on an existing installation also disables the built-in firewall after a reboot.

After a proper installation, the VPN Client does *not* show the stateful firewall under the options pulldown.

Using the VPN Client

- · To use the VPN Client, you need
 - Direct network connection (cable or DSL modem and network adapter/interface card), or
 - Internal or external modem
- To connect using a digital certificate for authentication, you need a digital certificate signed by one of the following Certificate Authorities (CAs) installed on your PC:
 - Baltimore Technologies (www.baltimoretechnologies.com)

- Entrust Technologies (www.entrust.com)
- Netscape (www.netscape.com)
- Verisign, Inc. (www.verisign.com)
- Microsoft Certificate Services Windows 2000
- A digital certificate stored on a smart card. The VPN Client supports smart cards via the MS CAPI Interface.

Advisories for Windows Vista Users

Windows Vista users should be aware of the following characteristics of the VPN Client.

Smart Card Support

The Cisco VPN Client for Windows Vista, Release 5.0.3.0560 and higher, supports Smart Card authentication (CSCsi25954).

Connection Time

Using the VPN Client to connect to a Windows Vista system might take longer than the time needed to connect to a Windows 2000 or Windows XP system. The actual time it takes to connect might vary from customer to customer.

Unsupported Features

The Cisco VPN Client for Windows Vista does *not* support the following features:

- System upgraded from Windows XP to Vista (clean OS installation required).
- Start Before Logon
- Integrated Firewall
- · InstallShield
- · 64-bit support
- AutoUpdate
- · Translated Online Help Provided only in English

API for Cisco VPN Client

The Cisco VPN Client offers an application programming interface (API). The software, sample program, and documentation are available at http://www.cisco.com/cgi-bin/tablebuild.pl/windows, along with the rest of the VPN Client downloads. The file name is APIExample_Rev4.zip.

If you do not have a CCO account, please visit http://tools.cisco.com/RPF/register/register.do and register for a guest account. Once you have done this forward the account ID to the vpn-client-api-support@cisco.com so that we can publish the file to you.



The Solaris VPN Client does not provide API support.

All API commands require that the 4.6.x and later of the VPN Client be fully installed.

If you are planning on using C, we recommend you call the vpnapi.dll directly; however, if you plan on using C++, then use the example provided in the zip file. The example is compatible with Visual Studio 2005. The documentation in the zip file works for both C & C++. There are no examples or support for C#, Visual Basic, or other programming languages. The existing example is not meant to be recompiled and will throw "safestring" missing errors if it is. Safestring is just a function to ensure proper strings, and it can either be replaced everywhere with another string function or rewritten.

Configuring the VPN Client

The procedures described in this section are common across all Cisco device platforms ("central-site devices") that the VPN Client connects to.

Configuring a Central-site Device for Remote Access Users

Before VPN Client users can access the remote network through a central-site device, you must complete the following tasks on the device:

- Complete all the steps in quick configuration, as a minimum.
- · Create and assign attributes to an IPsec group.
- Create and assign attributes to VPN Client users as members of the IPsec group.
- Configure VPN Client users who are using digital certificates instead of pre-shared keys for authentication.

Performing Quick Configuration

You can do quick configuration by using either default values for most of the setup parameters or specified values for specific parameters.

Quick Configuration Using Default Values

Quick configuration consists of the following steps:

- **Step 1** Configure the secure gateway Ethernet 1 interface to your private network.
- Step 2 Configure the other Ethernet interfaces that are connected to a public network or an additional external network.
- Step 3 Enter system identification information: system name, date, time, DNS, domain name, and default gateway.
- **Step 4** Specify tunneling protocols and encryption options.
- **Step 5** Specify methods for assigning IP addresses to clients as a tunnel is established.
- Step 6 Choose and identify the user authentication server: the internal server, RADIUS, NT Domain, SDI, or Kerberos/Active Directory.
- Step 7 If using the internal authentication server, populate the internal user database.
- Step 8 If using IPsec tunneling protocol, assign a name and password to the IPsec tunnel group.
- **Step 9** If using browser WebVPN, configure the WebVPN home page.

- **Step 10** Change the admin password for security.
- Step 11 Save the configuration file. When you complete this step, quick configuration is done.

Quick Configuration Using Non-default Values

Although you can choose to accept the default values, where applicable, for many of the quick configuration parameters, you can instead specify particular values for one or more of these parameters. The following table lists the parameters you need for quick configuration and provides space for you to record the values you enter. Write those values here now to save time as you enter data.

Table 1-2 Quick Configuration Parameters

Parameter Name	Parameter Description and Use	Your Entry
IP Interfaces > Ethernet 1 (Private)	Specify the IP address and subnet mask, speed, and duplex mode for the secure gateway interface to your private network.	
IP Interfaces > Ethernet 2 (Public)	Specify the IP address and subnet mask, speed, and duplex mode for the secure gateway interface to the public network.	
IP Interfaces > Ethernet 3 (External)	If so connected, specify the IP address and subnet mask, speed, and duplex mode for the secure gateway interface to an additional external network.	
System Info > System Name	Specify a device or system name for the secure gateway (for example, VPN01).	
System Info > DNS Server	Specify the IP address of your local DNS (Domain Name System) server.	
System Info > Domain	Specify the registered Internet domain name to use with DNS (for example, cisco.com).	
System Info > Default Gateway	Specify the IP address or hostname of the default gateway for packets not otherwise routed.	
Tunneling	Specify the tunneling method and encryption options you want to enable.	
Address Assignment > DHCP > Server	If you use Dynamic Host Configuration Protocol (DHCP) for remote address assignment, specify the IP address or hostname of the DHCP server.	
Address Assignment > Configured Pool > Range Start and Range End	If you use the secure gateway to assign addresses, specify the starting and ending IP addresses in its initial configured pool.	

Authentication	Your choice here determines the parameters you see in the following screen. Possible values are:	_
	Internal Server/Local	
	Choosing Internal Server, means using the internal VPN Concentrator user authentication server. On the User Database screen, specify the username and password for each user.	
	Additionally, if you specify per-user address assignment, specify the IP address and subnet mask for each user.	
	RADIUS	
	If you use an external RADIUS user authentication server, specify its IP address or hostname, port number, and server secret or password.	
	NT Domain	
	If you use an external Windows NT Domain user authentication server, specify its IP address, port number, and Primary Domain Controller hostname.	
	SDI	
	If you use an external SDI user authentication server, specify its IP address and port number.	
	Kerberos/Active Directory	
	If you use an external Kerberos/Active Directory authentication server, specify its IP address, port number, and realm.	
User Database > Group Name, Password, Verify	If you enable the IPsec tunneling protocol, specify a name and password for the IPsec tunnel group.	For security reasons, do not write your password here.
IPsec Group	Decide on a group name and password for the remote-access IPsec client.	
WebVPN	If you enable WebVPN, specify the default HTTPS, POP3S, SMTPS, or IMAP4S servers.	
WebVPN Home Page	If you enable WebVPN using HTTPS, configure the text and URLs that you want to appear on the WebVPN Home page.	

- Configure and enable both Ethernet interfaces 1 and 2 (Private and Public) with appropriate IP addresses and filters.
- Configure a DNS server and default gateway.
- Enable IPsec as one of the tunneling protocols (the default).
- Enter a group name and password for an IPsec group.

Configure at least one method for assigning user IP addresses.



If split or excluded tunnels are to be configured, ensure that the proper mask is assigned to the address pool or assigned IP address. By default, a classful mask is applied to the virtual adapter capable Clients, and this default mask might cause the Client to tunnel unintended traffic.

- Configure authentication servers for group and user authentication. These instructions assume the internal server for both, but you can set up any of the external servers instead.
- Save the configuration.

Configuring Entrust Entelligence for the VPN Client—Windows Only

This section explains how to set up a VPN Client to access Entrust Entelligence to obtain an Entrust identity certificate. It also provides information for using the VPN Client software with Entrust. For Entrust installation and configuration information, see your Entrust documentation—*Entrust Entelligence Quick Start Guide* or Entrust Entelligence online help.

Use the following procedure:

Step 1 Install Entrust Entelligence software on the remote user's PC.

You should install the Entrust Entelligence software before you install the VPN Client. The order is important when the VPN Client is using start before logon and Entrust SignOn at the same time. For information about what happens when both of these features are configured on the VPN Client, refer to *VPN Client User Guide for Windows*, Chapter 5.

Step 2 As part of Entust Entelligence installation, create a new Entrust profile, using the Create Entrust Profile Wizard.

To create an Entrust Entelligence profile, you need the following information:

- The Entrust Entelligence reference number
- The Entrust Entelligence authorization code
- The name of a directory for storing the profile
- A name for the profile
- · A password, following the rules set by the Entrust administrator
- Step 3 Optionally install Entrust SignOn, following the instructions in the Entrust documentation.
 - a. As part of Entrust SignOn installation, you see the Entrust Options dialog box. (See Figure 1-1.)
 - b. Make sure that you check **Always prompt me to confirm this login information**. Checking this box causes the Entrust SignOn login dialog box to pause and allow the VPN connection to come up before the remote user enters the logon information.

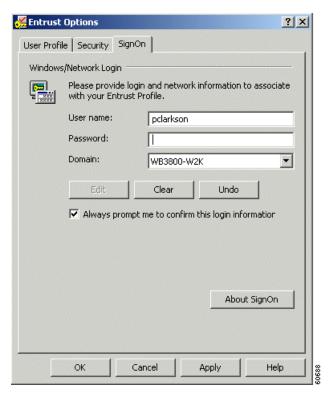


Figure 1-1 Entrust Options SignOn Tab

- **Step 4** After creating a profile, log out of Entrust Entelligence.
- Step 5 Install the VPN Client software.
- Step 6 Create a new connection entry that includes authenticating using an Entrust certificate. For instructions see section "Configuring an Entrust Certificate for Authentication," in Chapter 4 of VPN Client User Guide for Windows.



The VPN Client relies on an up-to-date Entrust DLL file. The name of this file is kmpapi32.dll. If you are using Entrust Entelligence version 5.1, the DLL file is up to date. If you have version 4.0 or 5.0 installed on the VPN Client system, then the DLL file is not up to date.

If "Entelligence Certificate (Entrust)" does not appear in the Certificate menu on the VPN Client, you probably do not have the latest version of the DLL file, which ships with the VPN Client software. To update the kmpapi32.dll file, copy it to the VPN Client system from the Release medium and place it in the Windows default system directory. For Windows Vista, Windows XP, this directory is c:\Windows\system32.

Setting up the VPN Client for Authentication using Smart Cards—Windows Only

The VPN Client supports authentication via a certificate stored on a smart card. After you create a connection entry and choose the certificate for authentication, the VPN Client user must insert the smart card into its reader. After the VPN Client connection is initiated, the user is prompted to enter a PIN or passcode to obtain access to the smart card. The private key stays on the smart card and is never accessible without entering the PIN or passcode. Also, in most cases, there is a limit to how many times someone can try to enter the PIN or passcode after which there is a lock on the card.

Explaining how to configure VPN Client authentication for every smart card vendor is beyond the scope of this documentation. You must follow documentation from your smart card vendor to obtain this information.

For example, using ASDM, do the following:

- Step 1 Under Key Options, when you are performing web-based certificate enrollment, choose your smart card provider from the pull-down menu.
- Step 2 For Key usage choose **Signature** and verify that **Create new key set** is selected.
- Step 3 Install the certificate. The keys are generated on the smart card and a copy of the certificate is stored in the Microsoft store on your PC and listed on the VPN Client Certificates tab.
- **Step 4** Modify the connection profile or tunnel group as follows:
 - a. Configure certificate authentication.
 - **b**. Enable the use of the smartcard certificate.

A VPN Client user can complete authentication only when the smart card is inserted in its reader that is plugged into the proper port on the PC and when the user enters the correct PIN or passcode.



With most vendors, when the smart card is not plugged in, the Certificates tab still displays the certificate. However when disconnected, e-token by Aladdin removes the certificate from the list. The certificate appears in the list only when the e-token is inserted and active.

Tear Down Tunnel When Smart Card Is Removed

When a smart card is removed from the system, the tunnel is automatically torn down. This causes the tunnel to immediately drop upon removal of the smart card from the system. This is an "always on" feature.

Notify User When a Smart Card Is Locked for Too Many Bad PINs

The VPN Client issues a log message when a smart card is blocked because too many incorrect PINs are entered. Under these circumstances, the connection eventually fails. The notification is a log message about the smart card being locked (CSCsb927).

Smart Card Password Reprompt for New Connections

Any time a new connection is made, the smart card requires the user to re-enter his or her credentials (password reprompt for new connections (uncache password)). The VPN Client does not allow connections to be re-established without the user re-entering the credentials to unlock the smart card.



It might be possible to bypass this feature and retain the behavior found in earlier VPN Client releases by adding an entry: BypassCardPinReset=1 in the vpnclient.ini file. However, this workaround does not work if the Smart Card Cryptographic Service Provider (CSP) ignores the cached PIN and prompts the user for PIN to access the private key (CSCsb73937).

Configuring Mutual Group Authentication

This section contains information to help an administrator configure authentication on a VPN Client system and on the central-site device. These notes apply to all VPN Client platforms.

Group Authentication is a method that uses pre-shared keys for mutual authentication. In this method, the VPN Client and the VPN central-site device use a group name and password to validate the connection. This is a symmetrical form of authentication since both sides use the same authentication method during their negotiations. Pre-shared authentication occurs in two stages.

During the first stage, the two sides exchange security parameters and create a secure channel. During the second stage, user authentication takes place. The VPN central-site device asks for username and password to verify that the remote user is a legitimate member of a group configured on the VPN central-site device.

Mutual group authentication is asymmetrical in that each side uses a different method to authenticate the other while establishing a secure tunnel to form the basis for group authentication. In this method, authentication happens in two stages. During the first stage, the VPN central-site device authenticates itself using public-key techniques (digital signature) and the two sides negotiate to establish a secure channel for communication. During the second stage, the actual authentication of the VPN Client user by the central-site VPN device takes place. since this approach does not use pre-shared keys for peer authentication, it provides greater security than group authentication alone as it is not vulnerable to a man-in-the-middle attack.

To use mutual group authentication, the remote user's VPN Client system must have a root certificate installed. If needed, you can install a root certificate automatically by placing it on the VPN Client system during installation. The certificate must be in a file named rootcert, with no extension and must be placed in the installation directory for the remote user's VPN Client system. For more information about loading a rootcert, see the installation instructions in the user guide for the remote user's platform.

Configuring IKE Parameters

This feature lets you set system wide values for VPN connections. The following sections describe each of the options.

Enabling IKE on Interfaces

You must enable IKE for each interface that you want to use for VPN connections.

Enabling IPsec over NAT-T

NAT-T lets IPsec peers establish both remote access and site-to-site connections through a NAT device. It does this by encapsulating IPsec traffic in UDP datagrams, using port 4500, thereby providing NAT devices with port information. NAT-T auto-detects any NAT devices, and only encapsulates IPsec traffic when necessary. This feature is disabled by default.

- The security appliance can simultaneously support standard IPsec, IPsec over TCP, NAT-T, and IPsec over UDP, depending on the client with which it is exchanging data.
- When both NAT-T and IPsec over UDP are enabled, NAT-T takes precedence.
- When enabled, IPsec over TCP takes precedence over all other connection methods.

The security appliance implementation of NAT-T supports IPsec peers behind a single NAT/PAT device as follows:

- One site-to-site connection.
- Either a site-to-site connection or multiple remote access clients, but not a mixture of both.

To use NAT-T you must:

- Open port 4500 on the security appliance.
- Enable IPsec over NAT-T globally in this panel.
- Select the appropriate option for the Fragmentation Policy. These options let traffic travel across NAT devices that do not support IP fragmentation; they do not impede the operation of NAT devices that do support IP fragmentation.

Enabling IPsec over TCP

IPsec over TCP enables a VPN client to operate in an environment in which standard ESP or IKE cannot function, or can function only with modification to existing firewall rules. IPsec over TCP encapsulates both the IKE and IPsec protocols within a TCP packet, and enables secure tunneling through both NAT and PAT devices and firewalls. This feature is disabled by default.



This feature does not work with proxy-based firewalls.

IPsec over TCP works with remote access clients. It works on all physical and VLAN interfaces. It is a client to security appliance feature only. It does not work for site-to-site connections.

- The security appliance can simultaneously support standard IPsec, IPsec over TCP, NAT-Traversal, and IPsec over UDP, depending on the client with which it is exchanging data.
- The VPN 3002 hardware client, which supports one tunnel at a time, can connect using standard IPsec, IPsec over TCP, NAT-Traversal, or IPsec over UDP.
- When enabled, IPsec over TCP takes precedence over all other connection methods.

You enable IPsec over TCP on both the security appliance and the client to which it connects.

You can enable IPsec over TCP for up to 10 ports that you specify. If you enter a well-known port, for example port 80 (HTTP) or port 443 (HTTPS), the system displays a warning that the protocol associated with that port will no longer work. The consequence is that you can no longer use a browser to manage the security appliance through the IKE-enabled interface. To solve this problem, reconfigure the HTTP/HTTPS management to different ports.

You must configure TCP port(s) on the client as well as on the security appliance. The client configuration must include at least one of the ports you set for the security appliance.

Determining ID Method

During IKE negotiations the peers must identify themselves to each other. You can choose the identification methods from the following options:

Table 1-3	IKE Identification Methods
Parameter	Use
Address	Uses the IP addresses of the hosts exchanging ISAKMP identity information.
Hostname	Uses the fully-qualified domain name of the hosts exchanging ISAKMP identity information (default). This name comprises the hostname and the domain name.
Key ID	Uses the string the remote peer uses to look up the preshared key.
Automatic	Determines IKE negotiation by connection type:
	IP address for preshared key
	Cert DN for certificate authentication.

Disabling Inbound Aggressive Mode Connections

Phase 1 IKE negotiations can use either Main mode or Aggressive mode. Both provide the same services, but Aggressive mode requires only two exchanges between the peers, rather than three. Aggressive mode is faster, but does not provide identity protection for the communicating parties. It is therefore necessary that they exchange identification information prior to establishing a secure SA in which to encrypt in formation. This feature is disabled by default.

Alerting Peers Before Disconnecting

Client or site-to-site sessions may be dropped for several reasons, such as: a security appliance shutdown or reboot, session idle timeout, maximum connection time exceeded, or administrator cut-off.

The security appliance can notify qualified peers (in site-to-site configurations), VPN Clients and VPN 3002 Hardware Clients of sessions that are about to be disconnected, and it conveys to them the reason. The peer or client receiving the alert decodes the reason and displays it in the event log or in a pop-up panel. This feature is disabled by default.

This panel lets you enable the feature so that the security appliance sends these alerts, and conveys the reason for the disconnect.

Qualified clients and peers include the following:

- Security appliance devices with Alerts enabled.
- VPN clients running 4.0 or later software (no configuration required).
- VPN 3002 hardware clients running 4.0 or later software, and with Alerts enabled.
- VPN 3000 Series Concentrators running 4.0 or later software, with Alerts enabled.

This feature does not apply to the following clients:

- Cisco AnyConnect VPN Client
- · Cisco IOS software
- Cisco Secure PIX Firewall

Special Considerations for Using IKE Keepalives

The ISAKMP (IKE) keepalive settings feature lets the security appliance monitor the continued presence of a remote peer and report its own presence to that peer. If the peer becomes unresponsive, the security appliance removes the connection. Enabling IKE keepalives prevents hung connections when the IKE peer loses connectivity.

There are various forms of IKE keepalives. For this feature to work, both the security appliance and its remote peer must support a common form. This feature works with the following peers:

- Cisco AnyConnect VPN Client
- Cisco VPN Client (Release 4.0 and above)
- Cisco VPN 3000 Client (Release 2.x)
- Cisco VPN 3002 Hardware Client
- Cisco VPN 3000 Series Concentrators
- · Cisco IOS software
- · Cisco Secure PIX Firewall

Non-Cisco VPN clients do not support IKE keepalives.

If you are configuring a group of mixed peers, and some of those peers support IKE keepalives and others do not, enable IKE keepalives for the entire group. The feature does not affect the peers that do not support it.

If you disable IKE keepalives, connections with unresponsive peers remain active until they time out, so we recommend that you keep your idle timeout short. You can change your idle timeout when you configure the group policy.



To reduce connectivity costs, disable IKE keepalives if this group includes any clients connecting via ISDN lines. ISDN connections normally disconnect if idle, but the IKE keepalive mechanism prevents connections from idling and therefore from disconnecting. If you do disable IKE keepalives, the client disconnects only when either its IKE or IPsec keys expire. Failed traffic does not disconnect the tunnel with the Peer Timeout Profile values as it does when IKE keepalives are enabled.

Waiting for Active Sessions to Terminate Prior to Reboot

You can schedule a central-site device reboot to occur only when all active sessions have terminated voluntarily. This feature is disabled by default.

The following procedure describes the general steps. See the specialized chapter for the environment you are using for the specific configuration parameters.

- Step 1 Enable IKE.
- **Step 2** Enable NAT transparency, if desired.

- Step 3 Specify the identity for this device to send to its peers. This lets you set the way that IPsec peers identify themselves to each other.
- **Step 4** Disable inbound aggressive mode connections—Select to disable aggressive mode connections.
- Step 5 Alert peers before disconnecting—Select to have the security appliance notify qualified site-to-site peers and remote access clients before disconnecting sessions.
- Step 6 Wait for all active sessions to voluntarily terminate before rebooting—Select to have the security appliance postpone a scheduled reboot until all active sessions terminate.



If you have a site-to-site configuration using IKE main mode, make sure that the two peers have the same IKE keepalive configuration. Both peers must have IKE keepalives enabled or both peers must have it disabled.

If you configure authentication using digital certificates, you can specify whether to send the entire certificate chain (which sends the peer the identity certificate and all issuing certificates) or just the issuing certificates (including the root certificate and any subordinate CA certificates).

You can notify users who are using outdated versions of Windows client software that they need to update their client, and you can provide a mechanism for them to get the updated client version. For VPN 3002 hardware client users, you can trigger an automatic update. You can configure and change the client-update, either for all connection profiles or for particular connection profiles.

If you configure authentication using digital certificates, you can specify the name of the trustpoint that identifies the certificate to send to the IKE peer.

Configuring VPN Client Firewall Policy for Windows

To provide a higher level of security, the VPN Client can either enforce the operation of a supported firewall or receive a pushed down stateful firewall policy for Internet bound traffic. This section includes the following topics:

- · How firewalls work with the VPN Client.
- List of the personal firewall products that the VPN Client can enforce for Internet traffic.
- How to configure a stateful firewall policy on a VPN Concentrator for the VPN Client to enforce.

Overview of Client Firewalls

This section summarizes how a network administrator can control personal firewall features from a secure gateway communicating policy information to the VPN Client running on a Windows platform.

Optional Versus Required Configuration Option

The secure gateway can require that a VPN Client use a designated firewall configuration or make this configuration optional. Making a designated firewall configuration optional gives a VPN Client user a chance to install the desired firewall on the client PC. When the VPN Client tries to connect, it notifies the secure gateway about any firewalls installed on the client PC. The secure gateway sends back

information about what firewall the VPN Client must use. If the firewall configuration is optional, the secure gateway can notify the VPN Client that there is a mismatch but still allow the VPN Client to establish a tunnel. The optional feature thus lets the network administrator of the VPN Client maintain the tunneled connection while obtaining and installing the required firewall.

Stateful Firewall (Always On)

The VPN Client configuration option Stateful Firewall (Always On) is enabled on the VPN Client. This configuration option is not negotiated. The policy is not controlled from the secure gateway. The VPN Client user enables this option on the VPN Client under the Options menu or while the VPN Client is active by right-clicking on the VPN Client icon and selecting the option.

When enabled, this feature allows no inbound sessions from all networks, whether or not a VPN connection is in effect. Also, the firewall is active for both tunneled and nontunneled traffic. Users who enable this feature cannot have a server running on their PC and their system can no longer respond to ping requests. There are two exceptions to allowing no inbound traffic. The first is DHCP, which sends requests to the DHCP server out one port but receives responses from DHCP through a different port. For DHCP, the stateful firewall allows inbound traffic. The second is ESP (VPN data). The stateful firewall allows ESP traffic from the secure gateway, because ESP rules are packet filters and not session-based filters.

Stateful Firewall (Always On) is the most basic VPN Client firewall and provides the highest level of security. However, it is also the least flexible, since it blocks almost all incoming traffic and does not allow outbound traffic to be limited.



The Always On personal firewall allows inbound access from the internal (tunneled) network to ensure that your internal applications work properly, while still providing additional protection for non tunneled traffic.

Cisco Integrated Client

The VPN Client on the Windows platform includes a stateful firewall that incorporates Zone Labs technology. This firewall is used for both the Stateful Firewall (Always On) feature and the Centralized Protection Policy (see "Centralized Protection Policy (CPP)"). This firewall is transparent to the VPN Client user, and is called "Cisco Integrated Client Firewall" or CIC. While the "Always On" option lets the VPN Client user choose to have basic firewall protection in effect, CPP lets an administrator define rules to enforce for inbound/outbound Internet traffic during split tunneling operation. Since tunnel everything already forces all traffic back through the tunnel, CPP is not used for tunnel everything.

Centralized Protection Policy (CPP)

Centralized Protection Policy (CPP) also known as firewall *push policy*, lets a network administrator define a set of rules for allowing or dropping Internet traffic while the VPN Client is tunneled in to the secure gateway. A network administrator defines this policy on the secure gateway, and the policy is sent to the VPN Client during connection negotiation. The VPN Client passes the policy to the Cisco Integrated Client, which then enforces the policy. If the client user has already selected the "Always On" option, any more restrictive rules are enforced for Internet traffic while the tunnel is established.

Since CIC includes a stateful firewall module, most configurations block all inbound traffic and permit either all outbound traffic or traffic through specific TCP and UDP ports outbound. Cisco Integrated Client, Zone Alarm, and Zone Alarm Pro firewalls can assign firewall rules. CPP rules are in effect

during split tunneling and help protect the VPN Client PC from Internet attacks by preventing servers from running and by blocking any inbound connections unless they are associated with outbound connections.

CPP provides more flexibility than the Stateful Firewall (Always On) feature, since with CPP, you can refine the ports and protocols that you want to permit.

Policy Configured on the Remote PC—Personal Firewall Enforcement

As an alternative to CPP, a network manager can define policy on the personal firewall that is installed on the same PC as the VPN Client. This approach accommodates situations where there is already a firewall set up and in use on the PC. The VPN Client then polls the personal firewall every 30 seconds to make sure it is running and if it is not, terminates the secure connection to the secure gateway. In this case, the secure gateway does not define the firewall policy. The only contact the VPN Client has with the firewall is polling it to ascertain that it is running, a capability known as Are You There (AYT).

Currently, the VPN Client supports the following personal firewalls:

- · BlackIce Defender
- Cisco Security Agent
- · Sygate Personal Firewall
- Sygate Personal Firewall Pro
- · Sygate Security Agent
- ZoneAlarm
- ZoneAlarmPro

Zone Labs Integrity Agent and Integrity Server (IA/IS)

The Zone Labs Integrity solution secures remote PCs on Windows platforms. This feature is a client/server solution that comprises four components:

- Integrity Server (IS)—located on a central organization's network, IS maintains policies for the firewall on the remote VPN Client PCs. A network manager defines the policy on the IS, the IS downloads the policy to the Integrity Agent (IA) on the remote PC through a secure tunnel activated through the VPN Concentrator. The IS monitors the PC to ensure enforcement of the policy. The IS also communicates with the secure gateway to establish/terminate connections, exchange session and user information, and report status information.
- Integrity Agent (IA)—on the remote PC enforces the protection policies it receives from IS and
 communicates with IS to exchange policy and status information. The IA also communicates with
 the VPN Client on the remote PC to obtain server addresses and to exchange status information with
 the secure gateway.
- Secure gateway—provides the means for configuring firewall functionality by group. It reports the
 IS's IP address and other VPN session-related information to the VPN Client, which passes it on to
 the IA. The secure gateway also communicates with the IS to establish and terminate sessions,
 exchange session and user information, and request and acquire authentication status.
- VPN Client—on the remote PC gets the IS addresses and information from the secure gateway and
 passes it to the IA. The VPN Client also gets and reports status information from the IA and
 terminates sessions.

After the connection is up and IS has communicated the firewall policy to IA, then IS and IA keep in touch though a heartbeat mechanism.

VPN Client for Linux Firewall Configuration

Cisco Systems provides the following firewall configuration, designed specifically for the VPN Client for Linux, Release 4.7.00.640, Virtual adapter. This code blocks all traffic on eth0, except for tunneled traffic.

```
# Firewall configuration written by Cisco Systems
# Designed for the Linux VPN Client 4.7.00.0640 Virtual Adapter
# Blocks ALL traffic on eth0 except for tunneled traffic
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
# Allow all traffic in both directions through the VA adapter
-A INPUT -i cipsec0 -j ACCEPT
-A OUTPUT -o cipsec0 -j ACCEPT
# Accept all encrypted VPN Client traffic in either direction on eth0
-A INPUT -i eth0 -p udp -s 0/0 --sport 500 -d 0/0 --dport 500 -j ACCEPT
-A OUTPUT -o eth0 -p udp -s 0/0 --sport 500 -d 0/0 --dport 500 -j ACCEPT
-A INPUT -i eth0 -p udp -s 0/0 --sport 4500 -d 0/0 --dport 4500 -j ACCEPT
-A OUTPUT -o eth0 -p udp -s 0/0 --sport 4500 -d 0/0 --dport 4500 -j ACCEPT
-A OUTPUT -o eth0 -p udp -s 0/0 --sport 1024: -d 0/0 --dport 29747 -j ACCEPT
# Block all other traffic in either direction on eth0
-A INPUT -i eth0 -j REJECT
-A OUTPUT -o eth0 -j REJECT
COMMIT
```

Setting up Local LAN Access for the VPN Client

Remote users with Cable or DSL access from home might have home networks for sharing files and printers. You can configure local LAN access for remote users so that they can access resources on the LAN at the client side and still maintain the secure connection to the central site (through the IPsec tunnel).

Before you begin, you should carefully read the section on split tunneling in the ASDM Online Help or ASDM User Guide, Cisco Adaptive Security Appliance Configuration Guide, or VPN 3000 Series Concentrator Reference Volume 1: Configuration

Configuring local LAN access involves the following general steps:

- Enabling local LAN access on the VPN Client
- Enabling local LAN access in specific groups on the VPN 3000 Concentrator
- Adding the accessible networks to a network list (or using the default network address).

Use the following procedure:

Step 1 On the VPN Client, enable the Allow Local LAN Access parameter.

When creating or modifying a connection entry, display the Transport tab and check **Allow Local LAN Access**.



Figure 1-2 Setting the Allow Local LAN Access Parameter on the VPN Client

- Step 2 On the secure gateway, either add a new group or modify an existing group as follows:
 - a. Configure the Split Tunneling Policy attribute as **Tunnel everything**, and then select **Allow the networks in list to bypass the tunnel**. This enables local LAN access on the VPN Client.
 - b. At the Split Tunneling Network List, select the network list you have created for local LAN access, if any.

VPN Client Local LAN is the default and is assigned the address 0.0.0.0/0.0.0.0. This IP address allows access to all hosts on the client side LAN without regard to the network addressing configured on that network. Since this local LAN access is limited to only one local network, if you have multiple network cards in the client PC, you can access only the network in which the VPN Client has established the VPN connection.

For information on creating a network list, see the ASDM Online Help, ASDM User Guide, *Cisco Adaptive Security Appliance Configuration Guide, or VPN 3000 Series Concentrator Reference Volume I: Configuration*, "Configuration | Policy Management | Traffic Management | Network Lists".



When the VPN Client is connected and configured for local LAN access, you cannot print or browse by name on the local LAN. When the VPN Client is disconnected, you can print or browse by name.

You can browse or print by IP Address. To print, you can change the properties for the network printer to use the IP Address instead of names. For example instead of the syntax \\sharename\printername, use \\x.x.x.x\printername, where x.x.x.x is an IP address.

To print and browse by name, you can use an LMHOSTS file. To do this, add the IP addresses and local hostnames to a text file named LMHOSTS and place it on all your local PCs in the \Windows directory. The PC's TCP/IP stack then uses the IP address to hostname mapping in the LMHOSTS file to resolve the name when printing or browsing. This approach requires that all local hosts have a static IP address; or if you are using DHCP, you must configure local hosts to always get the same IP address.

Example LMHOSTS file:

192.168.1.100 MKPC

192.168.1.101 SBPC

192.168.1.101 LHPC

Configuring Automatic Browser Configuration—Windows Only



This feature is supported only for Microsoft Internet Explorer web browser.

When a remote user connects to the a secure gateway, the VPN Client can receive a web browser proxy setting from the secure gateway and then change the web browser proxy configuration of the user to operate within the organization's environment. This setting is in effect only while the user is connected to the secure gateway. When the user disconnects, the VPN Client automatically changes the browser proxy of the PC to its original setting.

A network administrator configures this setting on the secure gateway.



The browser proxy feature in the VPN Client differs from Internet Explorer in the following ways:

In Internet Explorer, auto detect policy and use proxy server/port are not mutually exclusive. The VPN Client supports only a single proxy server for all protocols, while for Internet Explorer, you can configure a proxy server for each protocol.

The VPN Client does not support the Internet Explorer option "Use automatic configuration script."

Configuring the VPN Client on a Central-site Device

You can configure the VPN Client on a Cisco ASA 5500 Series Security Appliance, using either the Adaptive Security Device Manager (ASDM) or the command-line interface (CLI), or on a Cisco VPN 3000 Series Concentrator. The following chapters describe the procedures for each of these environments.



CHAPTER 2

Configuring the VPN Client Using ASDM

This chapter describes how to use the Adaptive Security Device Manager "ASDM) to configure the VPN Client on an Adaptive Security Appliance. It comprises the following sections:

- Configuring IPsec Remote Access Connection Profiles, page 2-1
- IKE Parameters, page 2-9
- Configuring Client Software Update Using ASDM, page 2-13
- Configuring Group Policies for IPsec Client Connections Using ASDM, page 2-16
- Configuring Advanced IPsec Client Parameters, page 2-20

Configuring IPsec Remote Access Connection Profiles

To configure the security appliance for use with the VPN Client, you must configure the appropriate parameters under Configuration > Remote Access VPN > Network (Client) Access > IPsec Connection Profiles, Group Policies, and Advanced.

This section describes the elements of the security appliance configuration process specifically relevant to the VPN Client. You must also configure (or accept the default values for) the rest of the parameters, as described in the ASDM online help, the ASDM User Manual, and the ASA CLI Configuration Guide.

The IPsec group uses the IPsec connection parameters to create a tunnel. An IPsec connection can be either remote-access or site-to-site. This chapter deals only with remote-access connections, though, for the sake of completeness, site-to-site connections are mentioned where appropriate. The IPsec group is configured on the internal server or on an external RADIUS server. For ASA 5505 in client mode or VPN 3002 hardware client parameters, which enable or disable interactive hardware client authentication and individual user authentication, the IPsec connection parameters take precedence over parameters set for users and groups.

If there are no connection profiles configured, or if you want to change an existing connection profile, click Add or Edit, as appropriate.



The terms "connection profile" and "tunnel group" are sometimes used interchangeably.

To configure IPsec connection profiles, select Configuration > Remote Access VPN > Network (Client) Access > IPsec Connection Profiles. The parameters in the IPsec Connection Profiles window let you configure IPsec remote access connections. Most of the parameters in this section were formerly configured under tunnel groups. An IPsec connection represents a connection-specific record for IPsec and Clientless SSL VPN connections. Perform the following steps:

- Step 1 In the Access Interfaces area, select the interfaces to enable for IPsec access. The default is that no access is selected.
- Step 2 The Connection Profiles area shows in tabular format the configured parameters for existing IPsec connections. The Connection Profiles s table contains records that determine connection policies. A record identifies a default group policy for the connection and contains protocol-specific connection parameters. The table contains the following columns:
 - Name—Specifies the name or IP address of the IPsec connection.
 - ID Certificate—Specifies the name of the ID certificate, if available.
 - IPsec Protocol—Indicates whether the IPsec protocol is enabled. You enable this protocol on the Add or Edit IPsec Remote Access Connection, Basic window.
 - L2TP/IPsec Protocol—Indicates whether the L2TP/IPsec protocol is enabled. You enable this protocol on the Add or Edit IPsec Remote Access Connection, Basic window.
 - Group Policy—Indicates the name of the group policy for this IPsec connection.
- Step 3 Select the IPsec Enabled check box to enable IPsec for each appropriate connection.

If you want to add a new connection profile or modify an existing, selected one, click Add or Edit. These open the Add or Edit IPsec Remote Access Connection Profile dialog box.

To remove the selected server group from the table, click Delete. There is no confirmation or undo.

Adding or Editing an IPsec Connection Profile

The Add or Edit IPsec Remote Access Connection Profile Basic dialog box lets you configure common attributes for IPsec connections. The navigation pane at the left of the dialog box lets you select whether you want to configure Basic or Advanced connection profile attributes.

Configuring Basic Attributes

Begin with the Basic attributes. The fields to configure are as follows:

Fields

- Name—Identifies the name of the connection. For the Edit function, this field is read-only.
- IKE Peer Authentication—Configures IKE peers.
 - Pre-shared key—Specifies the value of the pre-shared key for the connection. The maximum length of a pre-shared key is 128 characters.
 - Identity Certificate—Selects the name of an identity certificate, if any identity certificates are configured and enrolled.
 - Manage—Opens the Manage Identity Certificates window, on which you can add, edit, delete, export, and show details for a selected certificate.
- User Authentication—Specifies information about the servers used for user authentication. You can configure more authentication information in the Advanced section.

- Server Group—Selects the server group to use for user authentication, the default is LOCAL. If you select something other than LOCAL, the Fallback check box becomes available.
- Manage—Opens the Configure AAA Server Groups dialog box.
- Fallback—Specifies whether to use LOCAL for user authentication if the specified server group
- Client Address Assignment—Specifies attributes relevant to assigning client attributes.
 - DHCP Servers—Specifies the IP address of a DHCP server to use. You can add up to 10 servers, separated by spaces.
 - Client Address Pools—Specifies up to 6 predefined address pools. To define an address pool, go to Configuration > Remote Access VPN > Network Client Access > Address Assignment > Address Pools.
 - Select—Opens the Select Address Pools dialog box, on which you can select, add, or edit an address pool. Double-click your selection so that it appears in the Assigned Address Pools field. You can assign more than one address pool for a connection. When assigned, your selection appears in the Client Address Pools field.
- Default Group Policy—Specifies attributes relevant to the default group policy.
 - Group Policy—Selects the default group policy to use for this connection. The default is DfltGrpPolicy.
 - Manage—Opens the Configure Group Policies dialog box, from which you can add, edit, or delete group policies.
 - Client Protocols—Selects the protocol or protocols to use for this connection. By default, both IPsec and L2TP over IPsec are selected. Ensure that Enable IPsec protocol is selected.

Configuring Advanced Attributes

The Advanced attributes configure general, client addressing, authentication, authorization, accounting, IPsec, and PPP information for the connection profile. While you must configure (or accept the default values) for all the attributes, this section describes only those attributes that directly affect IPsec connections.

Configuring Client Addressing

To specify the client IP address assignment policy and assign address pools to all IPsec and SSL VPN connections, choose Configuration > Remote Access VPN > Network (Client) Access > IPsec or SSL VPN Connections > Add or Edit > Advanced > Client Addressing. The Add IPsec Remote Access Connection dialog box opens. Use this dialog box to add address pools and assign them to interfaces, and view, edit, or delete them. The table lists the configured interface-specific address pools.



Note

You cannot modify or remove an address pool if it is already in use. If you click Edit and the address pool is in use, ASDM displays an error message and lists the connection names and usernames that are using the addresses in the pool.

Use the following sections to understand and assign values to the fields in the Add IPsec Remote Access Connection window and its descendent windows:

Add or Edit IPsec Remote Access Connection and Add SSL VPN Access Connection, page 2-4

- Assigning Address Pools to an Interface, page 2-4
- Select Address Pools, page 2-5
- Add or Edit IP Pool, page 2-5

Add or Edit IPsec Remote Access Connection and Add SSL VPN Access Connection

To access the Add or Edit IPsec Remote Access Connection Profile window, choose Configuration > Remote Access VPN > Network (Client) Access > IPsec or SSL VPN Connections > Add or Edit > Advanced > Client Addressing.

Fields

Use the following descriptions to assign values to the fields in this window:

- Global Client Address Assignment Policy—Configures a policy that affects all IPsec and SSL VPN
 Client connections (including AnyConnect client connections). The security appliance uses the
 selected sources in order, until it finds an address:
 - Use authentication server—Specifies that the security appliance should attempt to use the authentication server as the source for a client address.
 - Use DHCP—Specifies that the security appliance should attempt to use DHCP as the source for a client address.
 - Use address pool—Specifies that the security appliance should attempt to use address pools as the source for a client address.
- Interface-Specific Address Pools—Lists the configured interface-specific address pools.
- Add or Edit—Opens the Assign Address Pools to Interface dialog box, on which you can view, add, or modify the address pool assignments, as described in the following section.
- Delete—Removes an address-pool assignment from the table.

Assigning Address Pools to an Interface

Use the Assign Address Pools to Interface window to select an interface and assign one or more address pools to that interface. To access this window, choose Configure > Remote Access VPN > Network (Client) Access > IPsec or SSL VPN Connections > Add or Edit > Advanced > Client Addressing > Add or Edit.

Fields

Use the following descriptions to assign values to the fields in this window:

- Interface—Select the interface to which you want to assign an address pool. The default is DMZ.
- Address Pools—Specify an address pool to assign to the specified interface.
- Select—Opens the Select Address Pools dialog box, on which you can select one or more address
 pools to assign to this interface. Your selection appears in the Address Pools field of the Assign
 Address Pools to Interface dialog box.

Select Address Pools

The Select Address Pools window shows the pool name, starting and ending addresses, and subnet mask of address pools available for client address assignment and lets you add, edit, or delete entries from that list. To access this window, choose Configuration > Remote Access VPN > Network (Client) Access > IPsec or SSL VPN Connections > Add or Edit > Advanced > Client Addressing > Add or Edit > Select.

Fields

Use the following descriptions to assign values to the fields in this window:

- Add—Opens the Add IP Pool window, on which you can configure a new IP address pool.
- · Edit—Opens the Edit IP Pool window, on which you can modify a selected IP address pool.
- Delete—Removes the selected address pool. There is no confirmation or undo.
- Assign—Displays the address pool names that remained assigned to the interface. Select a pool from
 the table and click Assign or double-click each unassigned pool you want to add to the interface.
 The Assign field updates the list of pool assignments on the Assign Address Pools to Interface dialog
 box.

Add or Edit IP Pool

The Add or Edit IP Pool dialog box lets you specify or modify a range of IP addresses for client address assignment. To access this dialog box, choose Configuration > Remote Access VPN > Network (Client) Access > IPsec or SSL VPN Connections > Add or Edit > Advanced > Client Addressing > Add or Edit > Select > Add or Edit.

Fields

Use the following descriptions to assign values to the fields in this window:

- Name—Specifies the name assigned to the IP address pool.
- Starting IP Address—Specifies the first IP address in the pool.
- Ending IP Address—Specifies the last IP address in the pool.
- Subnet Mask—Selects the subnet mask to apply to the addresses in the pool.

Configuring IPsec-specific Parameters

To configure IPsec-specific parameters, start by selecting Configuration > Remote Access VPN > Network (Client) Access > IPsec Connection Profiles, then do the following steps:

- Step 1 In the Access Interfaces area, check the appropriate boxes to enable specific interfaces for IPsec access. Only interfaces that have already been configured appear in this selection box.
- Step 2 In the Connection Profiles area, check the check box under IPsec Enabled for each connection profile (tunnel group) that uses IPsec.
- Step 3 To Add a connection profile to this list, click Add. You can then go back and configure all of the connection profile parameters. See Configuring IPsec Remote Access Connection Profiles, page 2-1 for details.

- Step 4 To modify an existing connection profile, click Edit. See Modifying an Existing IPsec Connection Profile, page 2-6.
- **Step 5** To remove a connection profile from this list, click Delete.
- **Step 6** Click Apply. The changes are saved to the running configuration.

Modifying an Existing IPsec Connection Profile

The Add or Edit IPsec Connection Profile window lets you configure or edit IPsec-specific connection-profile parameters, as previously described.

Fields

- Send certificate chain—Enables or disables sending the entire certificate chain. This action includes the root certificate and any subordinate CA certificates in the transmission.
- IKE Peer ID Validation—Selects whether IKE peer ID validation is ignored, required, or checked only if supported by a certificate.
- IKE Keep Alive—Enables and configures ISAKMP keep alive monitoring.
 - Disable Keep Alives—Enables or disables ISAKMP keep alives.
 - Monitor Keep Alives—Enables or disables ISAKMP keep alive monitoring. Selecting this
 option makes available the Confidence Interval and Retry Interval fields.
 - Confidence Interval—Specifies the ISAKMP keep alive confidence interval. This is the number
 of seconds the security appliance should allow a peer to idle before beginning keepalive
 monitoring. The minimum is 10 seconds; the maximum is 300 seconds. The default for a remote
 access group is 300 seconds.
 - Retry Interval—Specifies number of seconds to wait between ISAKMP keep alive retries. The default is 2 seconds.
 - Head end will never initiate keepalive monitoring—Specifies that the central-site security appliance never initiates keepalive monitoring.
- Interface-Specific Authentication Mode—Specifies the authentication mode on a per-interface basis.
 - Interface—Lets you select the interface name. The default interfaces are inside and outside, but if you have configured a different interface name, that name also appears in the list.
 - Authentication Mode—Lets you select the authentication mode, none, xauth, or hybrid, as above.
 - Interface/Authentication Mode table—Shows the interface names and their associated authentication modes that are selected.
 - Add or Edit—Adds or modifies an interface/authentication mode pair selection in the Interface/Authentication Modes table.
 - Delete—Removes an interface/authentication mode pair selection from the Interface/Authentication Modes table.
- Client VPN Software Update Table—Lists the client type, VPN Client revisions, and image URL
 for each client VPN software package installed. For each client type, you can specify the acceptable
 client software revisions and the URL or IP address from which to download software upgrades, if
 necessary. The client update mechanism (described in detail under the Client Update window) uses

this information to determine whether the software each VPN client is running is at an appropriate revision level and, if appropriate, to provide a notification message and an update mechanism to clients that are running outdated software.

Client Type—Identifies the VPN client type. "Windows" includes all Windows-based platforms. "Win NT" includes Windows Vista, Windows XP, Windows 2000, and Windows NT 4.0. The other platforms are Linux, Solaris, and Mac OS X. The VPN Client, release 5.0 and higher, does not support the Windows 95, Windows 98, and Windows ME platforms.



The secure gateway sends a separate notification message for each entry in a Client Update list; therefore, your client update entries must not overlap. For example, the value "Windows" includes all Windows platforms, and the value "WinNT" includes Windows Vista, Windows XP, Windows 2000, and Windows NT 4.0, so you cannot specify both Windows and Windows NT. To find out the client types and version information, click the lock icon in the top left corner of the Cisco Systems VPN Client main window and choose "About VPN Client."

- VPN Client Revisions—Specifies the acceptable revision level of the VPN client.
- Image URL—Specifies the URL or IP address from which the correct VPN client software image can be downloaded. For Windows-based VPN clients, the URL must be of the form http:// or https://. For ASA 5505 in client mode or VPN 3002 hardware clients, the URL must be of the form tftp://.

Configuring IKE Authentication Mode

Configure the default and interface-specific IKE authentication modes on the Configuration > Remote Access VPN > Network (Client) Access > IPsec Connection Profiles > Advanced > IPsec > IKE Authentication window by performing the following steps:

Step 1 Set the default mode: XAUTH, Hybrid XAUTH, or Disable user authentication during IKE.

- XAUTH—Specifies the use of IKE Extended Authentication mode, which provides the capability of authenticating a user within IKE using TACACS+ or RADIUS. This is the default value.
- Hybrid XAUTH—Specifies the use of Hybrid mode, which lets you use digital certificates for security appliance authentication and a different, legacy method—such as RADIUS, TACACS+ or SecurID—for remote VPN user authentication. This mode breaks phase 1 of the Internet Key Exchange (IKE) into the following steps, together called hybrid authentication:

The security appliance authenticates to the remote VPN user with standard public key techniques. This establishes an IKE security association that is unidirectionally authenticated.

An extended authentication (xauth) exchange then authenticates the remote VPN user. This extended authentication can use one of the supported legacy authentication methods.



Before setting the authentication type to hybrid, you must configure the authentication server and create a pre-shared key.

Disable user authentication during IKE—If you enable reauthentication on IKE rekey, the security
appliance prompts the user to enter a username and password during initial Phase 1 IKE negotiation
and also prompts for user authentication whenever an IKE rekey occurs. Reauthentication provides

additional security. If the configured rekey interval is very short, users might find the repeated authorization requests inconvenient. To avoid repeated authorization requests, disable reauthentication during IKE.

- Step 2 Specify whether to include the "Enter Username and Password" prompt in the XAUTH request.
- Step 3 To Add a connection profile to this list, click Add. To modify an existing connection profile, click Edit. To remove a connection profile from this list, click Delete.
- **Step 4** Click Apply. The changes are saved to the running configuration.

Adding or Editing a Connection Profile IKE Authentication Entry

Internet Key Exchange (IKE) establishes a shared security policy and authenticates keys for services (such as IPsec) that require keys. Before any IPsec traffic can be passed, each security appliance must verify the identity of its peer. This can be done by manually entering preshared keys into both hosts or by a CA service. IKE is a hybrid protocol that uses part Oakley and part of another protocol suite called SKEME inside the ISAKMP framework. This is the protocol formerly known as ISAKMP/Oakley, and is defined in RFC 2409.

You must enable IKE for each interface that you want to use for VPN connections.



VPN Client connections are not supported if you configure the **crypto isakmp keepalive** command with the periodic keyword (for example, **crypto isakmp keepalive timeoutval periodic**) on an IOS device.

IKE Extended Authenticate (XAUTH) is implemented per the IETF draft-ietf-ipsec-isakmp-xauth-04.txt ("extended authentication" draft). This protocol provides the capability of authenticating a user within IKE using TACACS+ or RADIUS.

Set the default mode for user authentication on the drop-down menu. The options are XAUTH (Extended user authentication), Hybrid XAUTH, and Disable user authentication during IKE. The default value is XAUTH.

XAUTH authenticates a user within IKE using TACACS+ or RADIUS. XAUTH authenticates a user using RADIUS or any of the other supported user authentication protocols.

Use hybrid XAUTH authentication when you need to use digital certificates for security appliance authentication and a different, legacy method for remote VPN user authentication, such as RADIUS, TACACS+ or SecurID.

Hybrid XAUTH breaks phase 1 of IKE down into the following two steps, together called hybrid authentication:

- The security appliance authenticates to the remote VPN user with standard public key techniques. This establishes an IKE security association that is unidirectionally authenticated.
- An XAUTH exchange then authenticates the remote VPN user. This extended authentication can use one of the supported legacy authentication methods.



Before setting the authentication type hybrid, you must configure the authentication server, create a preshared key, and configure a trustpoint.

To Add or Edit a specific interface on which to apply IKE authentication, do the following steps:

- Step 1 In the Interface-Specific Mode area, click Add or Edit. The Assign Authentication Mode to Interface dialog box appears.
- **Step 2** Select the interface from the drop-down menu.
- Step 3 Select the authentication mode to use. The choices are XAUTH, Hybrid XAUTH, and Disable user authentication during IKE, as explained above.
- **Step 4** Click OK. Your choices appear in the Interface-Specific Mode area.
- Step 5 Click OK to apply your selections.

IKE Parameters

To enable IKE parameters, select Configuration > Remote Access VPN This panel lets you set system wide values for VPN connections. The following sections describe each of the options.

Enabling IKE on Interfaces

You must enable IKE for each interface that you want to use for VPN connections.

Enabling IPsec over NAT-T

NAT-T lets IPsec peers establish both remote access and site-to-site connections through a NAT device. It does this by encapsulating IPsec traffic in UDP datagrams, using port 4500, thereby providing NAT devices with port information. NAT-T auto-detects any NAT devices, and only encapsulates IPsec traffic when necessary. This feature is disabled by default.

- The security appliance can simultaneously support standard IPsec, IPsec over TCP, NAT-T, and IPsec over UDP, depending on the client with which it is exchanging data.
- When both NAT-T and IPsec over UDP are enabled, NAT-T takes precedence.
- When enabled, IPsec over TCP takes precedence over all other connection methods.

The security appliance implementation of NAT-T supports IPsec peers behind a single NAT/PAT device as follows:

- One site-to-site connection.
- Either a site-to-site connection or multiple remote access clients, but not a mixture of both.

To use NAT-T you must:

- Open port 4500 on the security appliance.
- Enable IPsec over NAT-T globally in this panel.
- Select the second or third option for the Fragmentation Policy parameter in the Configuration > VPN > IPsec > Pre-Fragmentation panel. These options let traffic travel across NAT devices that do not support IP fragmentation; they do not impede the operation of NAT devices that do support IP fragmentation.

Enabling IPsec over TCP

IPsec over TCP enables a VPN client to operate in an environment in which standard ESP or IKE cannot function, or can function only with modification to existing firewall rules. IPsec over TCP encapsulates both the IKE and IPsec protocols within a TCP packet, and enables secure tunneling through both NAT and PAT devices and firewalls. This feature is disabled by default.



This feature does not work with proxy-based firewalls.

IPsec over TCP works with remote access clients. It works on all physical and VLAN interfaces. It is a client to security appliance feature only. It does not work for site-to-site connections.

- The security appliance can simultaneously support standard IPsec, IPsec over TCP, NAT-Traversal, and IPsec over UDP, depending on the client with which it is exchanging data.
- The VPN 3002 hardware client, which supports one tunnel at a time, can connect using standard IPsec, IPsec over TCP, NAT-Traversal, or IPsec over UDP.
- When enabled, IPsec over TCP takes precedence over all other connection methods.

You enable IPsec over TCP on both the security appliance and the client to which it connects.

You can enable IPsec over TCP for up to 10 ports that you specify. If you enter a well-known port, for example port 80 (HTTP) or port 443 (HTTPS), the system displays a warning that the protocol associated with that port will no longer work. The consequence is that you can no longer use a browser to manage the security appliance through the IKE-enabled interface. To solve this problem, reconfigure the HTTP/HTTPS management to different ports.

You must configure TCP port(s) on the client as well as on the security appliance. The client configuration must include at least one of the ports you set for the security appliance.

Determining ID Method

During IKE negotiations the peers must identify themselves to each other. You can choose the identification methods from the following options:

Table 2-1	IKE Identification Methods
Parameter	Use
Address	Uses the IP addresses of the hosts exchanging ISAKMP identity information.
Hostname	Uses the fully-qualified domain name of the hosts exchanging ISAKMP identity information (default). This name comprises the hostname and the domain name.
Key ID	Uses the string the remote peer uses to look up the preshared key.
Automatic	Determines IKE negotiation by connection type:
	IP address for preshared key
	Cert DN for certificate authentication.

Disabling Inbound Aggressive Mode Connections

Phase 1 IKE negotiations can use either Main mode or Aggressive mode. Both provide the same services, but Aggressive mode requires only two exchanges between the peers, rather than three. Aggressive mode is faster, but does not provide identity protection for the communicating parties. It is therefore necessary that they exchange identification information prior to establishing a secure SA in which to encrypt in formation. This feature is disabled by default.

Alerting Peers Before Disconnecting

Client or site-to-site sessions might be dropped for several reasons, such as: a security appliance shutdown or reboot, session idle timeout, maximum connection time exceeded, or administrator cut-off.

The security appliance can notify qualified peers (in site-to-site configurations), VPN Clients and VPN 3002 Hardware Clients of sessions that are about to be disconnected, and it conveys to them the reason. The peer or client receiving the alert decodes the reason and displays it in the event log or in a pop-up panel. This feature is disabled by default.

This panel lets you enable the feature so that the security appliance sends these alerts, and conveys the reason for the disconnect.

Qualified clients and peers include the following:

- · Security appliance devices with Alerts enabled.
- VPN clients running 4.0 or later software (no configuration required).
- VPN 3002 hardware clients running 4.0 or later software, and with Alerts enabled.
- VPN 3000 Series Concentrators running 4.0 or later software, with Alerts enabled.

This feature does not apply to the following clients:

- Cisco AnyConnect VPN Client
- · Cisco IOS software
- · Cisco Secure PIX Firewall

Waiting for Active Sessions to Terminate Prior to Reboot

You can schedule a central-site device reboot to occur only when all active sessions have terminated voluntarily. This feature is disabled by default.

Fields

- Enable IKE—Shows IKE status for all configured interfaces.
 - Interface—Displays names of all configured security appliance interfaces.
 - IKE Enabled—Shows whether IKE is enabled for each configured interface.
 - Enable/Disables—Click to enable or disable IKE for the highlighted interface.
- NAT Transparency—Lets you enable or disable IPsec over NAT-T and IPsec over TCP.
 - Enable IPsec over NAT-T—Select to enable IPsec over NAT-T.

- NAT Keepalive—Type the number of seconds that can elapse with no traffic before the security appliance terminates the NAT-T session. The default is 20 seconds. The range is 10 to 3600 seconds (one hour).
- Enable IPsec over TCP—Select to enable IPsec over TCP.
- Enter up to 10 comma-separated TCP port values—Type up to 10 ports on which to enable IPsec over TCP. Use a comma to separate the ports. You do not need to use spaces. The default port is 10,000. The range is 1 to 65,635.
- Identity to Be Sent to Peer—Lets you set the way that IPsec peers identify themselves to each other. During IKE negotiations the peers must identify themselves to each other. You can choose the identification methods from the following options:
 - Identity—Select one of the following methods by which IPsec peers identify themselves:

Parameter	Function
Address	Uses the IP addresses of the hosts.
Hostname	Uses the fully-qualified domain names of the hosts. This name comprises the hostname and the domain name.
Key ID	Uses the string the remote peer uses to look up the preshared key.
Automatic	Determines IKE negotiation by connection type: IP address for preshared key or cert DN for certificate authentication.

- Key Id String—Type the alphanumeric string the peers use to look up the preshared key.
- Disable inbound aggressive mode connections—Select to disable aggressive mode connections.
- Alert peers before disconnecting—Select to have the security appliance notify qualified site-to-site peers and remote access clients before disconnecting sessions.
- Wait for all active sessions to voluntarily terminate before rebooting—Select to have the security appliance postpone a scheduled reboot until all active sessions terminate.



If you have a site-to-site configuration using IKE main mode, make sure that the two peers have the same IKE keepalive configuration. Both peers must have IKE keepalives enabled or both peers must have it disabled.

If you configure authentication using digital certificates, you can specify whether to send the entire certificate chain (which sends the peer the identity certificate and all issuing certificates) or just the issuing certificates (including the root certificate and any subordinate CA certificates).

You can notify users who are using outdated versions of Windows client software that they need to update their client, and you can provide a mechanism for them to get the updated client version. For VPN 3002 hardware client users, you can trigger an automatic update. You can configure and change the client-update, either for all connection profiles or for particular connection profiles.

If you configure authentication using digital certificates, you can specify the name of the trustpoint that identifies the certificate to send to the IKE peer.

Configuring Client Software Update Using ASDM

The client update feature ensures acceptable Client revision levels. This feature lets administrators at a central location automatically notify VPN client users that it is time to update the VPN client software and the VPN 3002 hardware client image.

Remote users might be using outdated VPN software or hardware client versions. You can use the client-update feature to enable updating client revisions; specify the types and revision numbers of clients to which the update applies; provide a URL or IP address from which to get the update; and, in the case of Windows clients, optionally notify users that they should update their VPN client version. For Windows clients, you can provide a mechanism for users to accomplish that update. For VPN 3002 hardware client users, the update occurs automatically, with no notification. This feature applies only to the IPsec remote-access tunnel-group type.

If the client is already running a software version that is at least as high as those included on the list of revision numbers, it does not need to update its software. If the client is not running a software version on the list (or a higher version), it should update.

The Client VPN Software Update Table lists the client type, VPN Client revisions, and image URL for each client VPN software package installed. For each client type, you can specify the acceptable client software revisions and the URL or IP address from which to download software upgrades, if necessary. The client update mechanism (described in detail under the Client Update window) uses this information to determine whether the software each VPN client is running is at an appropriate revision level and, if appropriate, to provide a notification message and an update mechanism to clients that are running outdated software. Specify the following fields to configure client update.

Configure the Client Software Update Table on the Configuration > Remote Access VPN > Network (Client) Access > IPsec Connection Profiles > Advanced > IPsec > Client Software Update window by configuring the following fields:

Fields

- Enable Client Update—Enables or disables client update, both globally and for specific tunnel groups. You must enable client update before you can send a client update notification to Windows, MAC OS X, and Linux VPN clients, or initiate an automatic update to hardware clients.
- Client Type—Lists the clients to upgrade: software or hardware, and for Windows software clients, all Windows or a subset. If you click All Windows Based, do not specify Windows versions individually. The specification for Windows NT, Windows 2000, and Windows XP also includes Windows Vista. The hardware client gets updated with a release of the ASA 5505 software or of the VPN 3002 hardware client.

If the client update feature has already been configured to support all Windows clients, you must remove that specification before specifying individual Windows client types.



The secure gateway sends a separate notification message for each entry in a Client Update list; therefore, your client update entries must not overlap. For example, the value "Windows" includes all Windows platforms, and the value "WinNT" includes Windows Vista, Windows XP, Windows 2000, and Windows NT 4.0, so you cannot specify both Windows and Windows NT. To find out the client types and version information, click the lock icon in the top left corner of the Cisco Systems VPN Client main window and choose "About VPN Client."

- Client Type—Lists the clients to upgrade: software or hardware, and for Windows software clients, all Windows or a subset. If you click All Windows Based, do not specify Windows versions individually. The specification for Windows NT, Windows 2000, and Windows XP also includes Windows Vista. The hardware client gets updated with a release of the ASA 5505 software or of the VPN 3002 hardware client.
- VPN Client Revisions—Contains a comma-separated list of software image revisions appropriate for this client. If the user's client revision number matches one of the specified revision numbers, there is no need to update the client, and, for Windows-based clients, the user does not receive an update notification. The following caveats apply:
 - The revision list must include the software version for this update.
 - Your entries must match exactly those on the URL for the VPN client, or the TFTP server for the hardware client.
 - The TFTP server for distributing the hardware client image must be a robust TFTP server.
 - A VPN client user must download an appropriate software version from the listed URL.
 - The VPN 3002 hardware client software is automatically updated via TFTP, with no notification to the user.
- Image URL—Contains the URL or IP address from which to download the software image. This URL must point to a file appropriate for this client. For Windows, MAC OS X, and Linux-based clients, the URL must be in the form: http:// or https://. For hardware clients, the URL must be in the form tftp://.
 - For Windows, MAC OS X, and Linux-based VPN clients: To activate the Launch button on the VPN Client Notification, the URL must include the protocol HTTP or HTTPS and the server address of the site that contains the update. The format of the URL is: http(s)://server_address:port/directory/filename. The server address can be either an IP address or a hostname if you have configured a DNS server. For example:

```
http://10.10.99.70/vpnclient-win-4.6.Rel-k9.exe
```

The directory is optional. You need the port number only if you use ports other than 80 for HTTP or 443 for HTTPS.

 For the hardware client: The format of the URL is tftp://server_address/directory/filename. The server address can be either an IP address or a hostname if you have configured a DNS server.
 For example:

```
tftp://10.1.1.1/vpn3002-4.1.Rel-k9.bin
```

Enabling Client Update

To enable IPsec VPN Client update and, optionally, upgrade connected clients, select Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Upload Software > Client Software.

The Client Software dialog box lets administrators at a central location do the following actions:

- Enable client update; specify the types and revision numbers of clients to which the update applies.
- Provide a URL or IP address from which to get the update.
- In the case of Windows clients, optionally notify users that they should update their VPN client version.



The Client Update function at Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Upload Software > Client Software applies only to the (IPsec) Cisco VPN Client, (for Windows, MAC OS X, and Linux), and the VPN 3002 hardware client. It does not apply to the Cisco AnyConnect VPN clients, which is automatically updated by the security appliance when it connects.

For the IPsec VPN Client, you can provide a mechanism for users to accomplish that update. For VPN 3002 hardware client users, the update occurs automatically, with no notification. You can apply client updates only to the IPsec remote-access tunnel-group type.



If you try to do a client update to an IPsec site-to-site IPsec connection or a Clientless VPN IPsec connection, you do not receive an error message, but no update notification or client update goes to those types of IPsec connections.

To enable client update globally for all clients of a particular client type, use this window. You can also notify all Windows, MAC OS X, and Linux clients that an upgrade is needed and initiate an upgrade on all VPN 3002 hardware clients from this window. To configure the client revisions to which the update applies and the URL or IP address from which to download the update, click Edit.

To configure client update revisions and software update sources for a specific tunnel group, see Configuration > Remote Access VPN > Network (Client) Access > IPsec > Add/Edit > Advanced > IPsec > Client Software Update.

Fields

- Enable Client Update—Enables or disables client update, both globally and for specific tunnel groups. You must enable client update before you can send a client update notification to Windows, MAC OS X, and Linux VPN clients, or initiate an automatic update to hardware clients.
- Client Type—Lists the clients to upgrade: software or hardware, and for Windows software clients, all Windows or a subset. If you click All Windows Based, do not specify Windows versions individually. The hardware client gets updated with a release of the ASA 5505 software or of the VPN 3002 hardware client.



Note

The secure gateway sends a separate notification message for each entry in a Client Update list; therefore, your client update entries must not overlap. For example, the value "Windows" includes all Windows platforms, and the value "WinNT" includes Windows Vista, Windows XP, Windows 2000, and Windows NT 4.0, so you cannot specify both Windows and Windows NT. To find out the client types and version information, click the lock icon in the top left corner of the Cisco Systems VPN Client main window and choose "About VPN Client."

- VPN Client Revisions—Contains a comma-separated list of software image revisions appropriate for this client. If the user's client revision number matches one of the specified revision numbers, there is no need to update the client, and, for Windows-based clients, the user does not receive an update notification. The following caveats apply:
 - The revision list must include the software version for this update.
 - Your entries must match exactly those on the URL for the VPN client, or the TFTP server for the hardware client.
 - The TFTP server for distributing the hardware client image must be a robust TFTP server.
 - A VPN client user must download an appropriate software version from the listed URL.

- The VPN 3002 hardware client software is automatically updated via TFTP, with no notification to the user.
- Image URL—Contains the URL or IP address from which to download the software image. This URL must point to a file appropriate for this client. For Windows, MAC OS X, and Linux-based clients, the URL must be in the form: http:// or https://. For hardware clients, the URL must be in the form tftp://.
 - For Windows, MAC OS X, and Linux-based VPN clients: To activate the Launch button on the VPN Client Notification, the URL must include the protocol HTTP or HTTPS and the server address of the site that contains the update. The format of the URL is: http(s)://server_address:port/directory/filename. The server address can be either an IP address or a hostname if you have configured a DNS server. For example:

```
http://10.10.99.70/vpnclient-win-4.6.Rel-k9.exe
```

The directory is optional. You need the port number only if you use ports other than 80 for HTTP or 443 for HTTPS.

For the hardware client: The format of the URL is tftp://server_address/directory/filename. The server address can be either an IP address or a hostname if you have configured a DNS server. For example:

```
tftp://10.1.1.1/vpn3002-4.1.Rel-k9.bin
```

- Edit—Opens the Edit Client Update Entry dialog box, which lets you configure or change client update parameters. See Edit Client Update Entry.
- Live Client Update—Sends an upgrade notification message to all currently connected VPN clients or selected tunnel group(s).
 - Tunnel Group—Selects all or specific tunnel group(s) for updating.
 - Update Now—Immediately sends an upgrade notification containing a URL specifying where to retrieve the updated software to the currently connected VPN clients in the selected tunnel group or all connected tunnel groups. The message includes the location from which to download the new version of software. The administrator for that VPN client can then retrieve the new software version and update the VPN client software.

For VPN 3002 hardware clients, the upgrade proceeds automatically, with no notification.

You must check Enable Client Update in the window for the upgrade to work. Clients that are not connected receive the upgrade notification or automatically upgrade the next time they log on.

Configuring Group Policies for IPsec Client Connections Using ASDM

The Group Policies window, Configuration > Remote Access VPN > Network (Client) Access > Group Policies) lets you manage the attributes for individual VPN group policies. A VPN group policy is a collection of user-oriented attribute/value pairs stored either internally on the device or externally on a RADIUS or LDAP server. Configuring the VPN group policy lets users inherit attributes that you have not configured at the individual group or username level. By default, VPN users have no group policy association. The group policy information is used by VPN tunnel groups and user accounts.

The "child" windows and dialog boxes let you configure the group parameters, including those for the default group. The default group parameters are those that are most likely to be common across all groups and users, and they streamline the configuration task. Groups can "inherit" parameters from this default group, and users can "inherit" parameters from their group or the default group. You can override these parameters as you configure groups and users.

You can configure either an internal or an external group policy. An internal group policy is stored locally, and an external group policy is stored externally on a RADIUS or LDAP server. Clicking Edit opens a similar dialog box on which you can create a new group policy or modify an existing one.

In these dialog boxes, you configure the following kinds of parameters:

- General attributes: Name, banner, address pools, protocols, filtering, and connection settings.
- Servers: DNS and WINS servers, DHCP scope, and default domain name.
- Advanced attributes: Split tunneling, IE browser proxy, SSL VPN Client and AnyConnect Client, and IPsec Client.

Before configuring these parameters, you should configure the following:

- · Access hours.
- Rules and filters.
- IPsec Security Associations.
- · Network lists for filtering and split tunneling
- User authentication servers, and specifically the internal authentication server.

Fields

- Group Policy—Lists the currently configured group policies and Add, Edit, and Delete buttons to help you manage VPN group policies.
- Name—Lists the name of the currently configured group policies.
- Type—Lists the type of each currently configured group policy.
- Tunneling Protocol—Lists the tunneling protocol that each currently configured group policy uses.
- AAA Server Group—Lists the AAA server group, if any, to which each currently configured group
 policy pertains.
- Add—Offers a drop-down menu on which you can select whether to add an internal or an external group policy. If you simply click Add, then by default, you create an internal group policy. Clicking Add opens the Add Internal Group Policy dialog box or the Add External Group Policy dialog box, which let you add a new group policy to the list. This dialog box includes three menu sections. Click each menu item to display its parameters. As you move from item to item, ASDM retains your settings. When you have finished setting parameters on all menu sections, click Apply or Cancel.Offers a drop-down menu on which you can select whether to add an internal or an external group policy. If you simply click Add, then by default, you create an internal group policy.
- Edit—Displays the Edit Group Policy dialog box, which lets you modify an existing group policy.
- Delete—Lets you remove a AAA group policy from the list. There is no confirmation or undo.

Adding or Editing a Remote Access Internal Group Policy, General Attributes

The Add or Edit Group Policy dialog box lets you specify tunneling protocols, filters, connection settings, and servers for the group policy being added or modified. For each of the fields on this window, checking the Inherit check box lets the corresponding setting take its value from the default group policy. Inherit is the default value for all of the attributes on this dialog box.



The fields most important for the VPN Client appear below the More Options line. You must select IPsec as one of the tunneling protocols unless you are certain that the individual group policy or username from which this group would inherit specifies IPsec as the tunneling protocol.

Fields

The following attributes appear in the Add or Edit Internal Group Policy > General dialog box. They apply to SSL VPN and IPsec sessions, or clientless SSL VPN sessions. Thus, several are present for one type of session, but not the other.

- Name—Specifies the name of this group policy. For the Edit function, this field is read-only.
- Banner—Specifies the banner text to present to users at login. The length can be up to 491 characters. There is no default value.
- Address Pools—(Network (Client) Access only) Specifies the name of one or more address pools to
 use for this group policy. You configure the address pools by selecting Configuration > Remote
 Access VPN > Network (Client) Access > Address Assignment > Address Pools.
- Select—(Network (Client) Access only) Opens the Select Address Pools window, which shows the pool name, starting and ending addresses, and subnet mask of address pools available for client address assignment and lets you select, add, edit, delete, and assign entries from that list.
- More Options—Displays additional configurable options for this group policy.
- Tunneling Protocols—Specifies the tunneling protocols that this group can use. Users can use only
 the selected protocols. The choices are as follows:
 - Clientless SSL VPN—Specifies the use of VPN via SSL/TLS, which uses a web browser to establish a secure remote-access tunnel to a security appliance; requires neither a software nor hardware client. Clientless SSL VPN can provide easy access to a broad range of enterprise resources, including corporate websites, web-enabled applications, NT/AD file share (web-enabled), e-mail, and other TCP-based applications from almost any computer that can reach HTTPS Internet sites.
 - SSL VPN Client—Specifies the use of the Cisco AnyConnect VPN client or the legacy SSL VPN client.
 - IPsec—IP Security Protocol. Regarded as the most secure protocol, IPsec provides the most complete architecture for VPN tunnels. Both site-to-site (peer-to-peer) connections and client-to-LAN connections can use IPsec.
 - L2TP over IPsec—Allows remote users with VPN clients provided with several common PC and mobile PC operating systems to establish secure connections over the public IP network to the security appliance and private corporate networks. L2TP uses PPP over UDP (port 1701) to tunnel the data. The security appliance must be configured for IPsec transport mode.



If you do not select a protocol, an error message appears.

- Filter—(Network (Client) Access only) Specifies which access control list to use, or whether to
 inherit the value from the group policy. Filters consist of rules that determine whether to allow or
 reject tunneled data packets coming through the security appliance, based on criteria such as source
 address, destination address, and protocol. To configure filters and rules, see the Group Policy
 window.
- Web ACL—(Clientless SSL VPN only) Select an access control list (ACL) from the drop-down list
 if you want to filter traffic. Click Manage next to the list if you want to view, modify, add, or remove
 ACLs before making a selection.
- Manage—Displays the ACL Manager window, with which you can add, edit, and delete Access
 Control Lists (ACLs) and Extended Access Control Lists (ACEs). For more information about the
 ACL Manager, see the online Help for that window.
- NAC Policy—Selects the name of a Network Admission Control policy to apply to this group policy. You can assign an optional NAC policy to each group policy. The default value is --None--.
- Manage—Opens the Configure NAC Policy dialog box. After configuring one or more NAC
 policies, the NAC policy names appear as options in the drop-down list next to the NAC Policy
 attribute.
- Access Hours—Selects the name of an existing access hours policy, if any, applied to this user or
 create a new access hours policy. The default value is Inherit, or, if the Inherit check box is not
 selected, the default value is --Unrestricted--.
- Manage—Opens the Browse Time Range dialog box, on which you can add, edit, or delete a time range.
- Simultaneous Logins—Specifies the maximum number of simultaneous logins allowed for this user. The default value is 3. The minimum value is 0, which disables login and prevents user access.



Note

While there is no maximum limit, allowing several simultaneous connections might compromise security and affect performance.

• Restrict Access to VLAN—(Optional) Also called "VLAN mapping," this parameter specifies the egress VLAN interface for sessions to which this group policy applies. The security appliance forwards all traffic on this group to the selected VLAN. Use this attribute to assign a VLAN to the group policy to simplify access control. Assigning a value to this attribute is an alternative to using ACLs to filter traffic on a session. In addition to the default value (Unrestricted), the drop-down list shows only the VLANs that are configured on this security appliance.



Note

This feature works for HTTP connections, but not for FTP and CIFS.

- Maximum Connect Time—If the Inherit check box is not selected, this parameter specifies the
 maximum user connection time in minutes. At the end of this time, the system terminates the
 connection. The minimum is 1 minute, and the maximum is 35791394 minutes (over 4000 years).
 To allow unlimited connection time, select Unlimited (the default).
- Idle Timeout—If the Inherit check box is not selected, this parameter specifies this user's idle timeout period in minutes. If there is no communication activity on the user's connection in this period, the system terminates the connection. The minimum time is 1 minute, and the maximum time is 10080 minutes. The default is 30 minutes. To allow unlimited connection time, select Unlimited. This value does not apply to Clientless SSL VPN users.

• On smart card removal—With the default option, Disconnect, the client tears down the connection if the smart card used for authentication is removed. Click Keep the connection if you do not want to require users to keep their smart cards in the computer for the duration of the connection.

Configuring Advanced IPsec Client Parameters

The Add or Edit Group Policy > Advanced > IPsec Client dialog box lets you specify tunneling protocols, filters, connection settings, and servers for the group policy being added or modified.

Fields

- Re-Authentication on IKE Re-key—Enables or disables reauthentication when IKE re-key occurs, unless the Inherit check box is selected. The user has 30 seconds to enter credentials, and up to three attempts before the SA expires at approximately two minutes and the tunnel terminates.
- Enable extended reauth-on-rekey to allow entry of authentication credentials until SA
 expiry—Allow users the time to reenter authentication credentials until the maximum lifetime of the
 configured SA.
- IP Compression—Enables or disables IP Compression, unless the Inherit check box is selected.
- Perfect Forward Secrecy—Enables or disables perfect forward secrecy (PFS), unless the Inherit check box is selected. PFS ensures that the key for a given IPsec SA was not derived from any other secret (like some other keys). In other words, if someone were to break a key, PFS ensures that the attacker would not be able to derive any other key. If PFS were not enabled, someone could hypothetically break the IKE SA secret key, copy all the IPsec protected data, and then use knowledge of the IKE SA secret to compromise the IPsec SAs set up by this IKE SA. With PFS, breaking IKE would not give an attacker immediate access to IPsec. The attacker would have to break each IPsec SA individually.
- Store Password on Client System—Enables or disables storing the password on the client system.



Storing the password on a client system can constitute a potential security risk.

- IPsec over UDP—Enables or disables using IPsec over UDP.
- IPsec over UDP Port—Specifies the UDP port to use for IPsec over UDP.
- Tunnel Group Lock—Enables locking the tunnel group you select from the list, unless the Inherit check box or the value None is selected.
- IPsec Backup Servers—Activates the Server Configuration and Server IP Addresses fields, so you
 can specify the UDP backup servers to use if these values are not inherited.
 - Server Configuration—Lists the server configuration options to use as an IPsec backup server.
 The available options are: Keep Client Configuration (the default), Use the Backup Servers Below, and Clear Client Configuration.
 - Server Addresses (space delimited)—Specifies the IP addresses of the IPsec backup servers.
 This field is available only when the value of the Server Configuration selection is Use the Backup Servers Below.

Configuring Client Access Rules

The Add or Edit Group Policy > Advanced > IPsec Client > Client Access Rules dialog box lets you permit or deny access by certain types and versions of VPN Clients. If you do not define any rules, the security appliance permits all client types. If a client matches none of the rules, the security appliance denies the connection. If you define a deny rule, you must also define at least one permit rule, or the security appliance denies all connections for the group policy being added or modified.

Adding or Editing Client Access Rules

The Add or Edit Client Access Rule dialog box adds a new client access rule for an IPsec group policy or modifies an existing rule. The fields on this dialog box relate to various types of VPN clients, so be aware that not all of the possible values are valid for the IPsec VPN Client.

Fields

- · Priority—Shows the priority for this rule.
- Action—Specifies whether this rule permits or denies access.
- VPN Client Type—Specifies the type of VPN client to which this rule applies, software or hardware, and for software clients, all Windows clients or a subset. Some common values for VPN Client Type include VPN 3002, PIX, Linux, * (matches all client types), and WinNT (matches Windows NT, Windows 2000, Windows XP, and Windows Vista). If you choose *, do not configure individual Windows types such as Windows XP.
- VPN Client Version—Specifies the version or versions of the VPN client to which this rule applies.
 This box contains a comma-separated list of software or firmware images appropriate for this client.
- The following caveats apply:
 - You must specify the software version for this client. You can specify * to match any version.
 - Your entries must match exactly those on the URL for the VPN client, or the TFTP server for the VPN 3002.
 - The TFTP server for distributing the hardware client image must be a robust TFTP server.
 - If the client is already running a software version on the list, it does not need a software update.
 If the client is not running a software version on the list, an update is in order.
 - A VPN Client user must download an appropriate software version from the listed URL.
 - The VPN 3002 hardware client software is automatically updated via TFTP.

Configuring Client Firewall Parameters

The Add or Edit Group Policy > Advanced > IPsec Client > Client Firewall dialog box lets you set personal firewall policies for VPN Clients for the group policy being added or modified. The security appliance pushes this firewall policy to the VPN client during connection setup negotiation. If you have users in this group who do not yet have a firewall, choose "Firewall Optional" in the Firewall Setting field.



Only VPN clients running Microsoft Windows can use these firewall features. These features are currently not available to hardware clients or other (non-Windows) software clients.

A firewall isolates and protects a computer from the Internet by inspecting each inbound and outbound individual packet of data to determine whether to allow or drop it. Firewalls provide extra security if remote users in a group have split tunneling configured. In this case, the firewall protects the user's PC, and thereby the corporate network, from intrusions by way of the Internet or the user's local LAN. Remote users connecting to the security appliance with the VPN client can choose the appropriate firewall option.

In the first scenario, a remote user has a personal firewall installed on the PC. The VPN client enforces firewall policy defined on the local firewall, and it monitors that firewall to make sure it is running. If the firewall stops running, the VPN client drops the connection to the security appliance. (This firewall enforcement mechanism is called Are You There (AYT), because the VPN client monitors the firewall by sending it periodic "are you there?" messages; if no reply comes, the VPN client knows the firewall is down and terminates its connection to the security appliance.) The network administrator might configure these PC firewalls originally, but with this approach, each user can customize his or her own configuration.

In the second scenario, you might prefer to enforce a centralized firewall policy for personal firewalls on VPN client PCs. A common example would be to block Internet traffic to remote PCs in a group using split tunneling. This approach protects the PCs, and therefore the central site, from intrusions from the Internet while tunnels are established. This firewall scenario is called push policy or Central Protection Policy (CPP). On the security appliance, you create a set of traffic management rules to enforce on the VPN client, associate those rules with a filter, and designate that filter as the firewall policy. The security appliance pushes this policy down to the VPN client. The VPN client then in turn passes the policy to the local firewall, which enforces it.

Fields

- Inherit—Determines whether the group policy obtains its client firewall setting from the default group policy. This option is the default setting. When set, it overrides the remaining attributes in this tab and dims their names.
- Firewall Setting—Lists whether a firewall exists, and if so, whether it is required or optional. If you select No Firewall (the default), none of the remaining fields on this window are active. If you want users in this group to be firewall-protected, select either the Firewall Required or Firewall Optional setting.

If you select Firewall Required, all users in this group must use the designated firewall. The security appliance drops any session that attempts to connect without the designated, supported firewall installed and running. In this case, the security appliance notifies the VPN client that its firewall configuration does not match.



Note If you require a firewall for a group, make sure the group does not include any clients other than Windows VPN clients. Any other clients in the group (including ASA 5505 in client mode and VPN 3002 hardware clients) are unable to connect.

If you have remote users in this group who do not yet have firewall capacity, choose Firewall Optional. The Firewall Optional setting allows all the users in the group to connect. Those who have a firewall can use it; users that connect without a firewall receive a warning message. This setting is useful if you are creating a group in which some users have firewall support and others do not—for example, you may have a group that is in gradual transition, in which some members have set up firewall capacity and others have not yet done so.

- Firewall Type—Lists firewalls from several vendors, including Cisco. If you select Custom Firewall, the fields under Custom Firewall become active. The firewall you designate must correlate with the firewall policies available. The specific firewall you configure determines which firewall policy options are supported.
- Custom Firewall—Specifies the vendor ID, Product ID and description for the custom firewall.
 - Vendor ID—Specifies the vendor of the custom firewall for this group policy.
 - Product ID—Specifies the product or model name of the custom firewall being configured for this group policy.
 - Description—(Optional) Describes the custom firewall.
- Firewall Policy—Specifies the type and source for the custom firewall policy.
 - Policy defined by remote firewall (AYT)—Specifies that the firewall policy is defined by the remote firewall (Are You There). Policy defined by remote firewall (AYT) means that remote users in this group have firewalls located on their PCs. The local firewall enforces the firewall policy on the VPN client. The security appliance allows VPN clients in this group to connect only if they have the designated firewall installed and running. If the designated firewall is not running, the connection fails. Once the connection is established, the VPN client polls the firewall every 30 seconds to make sure that it is still running. If the firewall stops running, the VPN client ends the session.
 - Policy pushed (CPP)—Specifies that the policy is pushed from the peer. If you select this option, the Inbound Traffic Policy and Outbound Traffic Policy lists and the Manage button become active. The security appliance enforces on the VPN clients in this group the traffic management rules defined by the filter you choose from the Policy Pushed (CPP) drop-down menu. The choices available on the menu are filters defined on this security appliance, including the default filters. Keep in mind that the security appliance pushes these rules down to the VPN client, so you should create and define these rules relative to the VPN client, not the security appliance. For example, "in" and "out" refer to traffic coming into the VPN client or going outbound from the VPN client. If the VPN client also has a local firewall, the policy pushed from the security appliance works with the policy of the local firewall. Any packet that is blocked by the rules of either firewall is dropped.
 - Inbound Traffic Policy—Lists the available push policies for inbound traffic.
 - Outbound Traffic Policy—Lists the available push policies for outbound traffic.
- Manage—Displays the ACL Manager window, on which you can configure Access Control Lists (ACLs).

Configuring Hardware Client Parameters

You do not configure these parameters for the VPN Client. Configure the hardware client parameters on the Add or Edit Group Policy > Advanced > IPsec Client > Hardware Client dialog box only if you are configuring a hardware client such as the ASA 5505 used as a hardware client.

Configuring Advanced IPsec Client Parameters



 $_{\sf chapter}\,3$

Configuring VPN Client Parameters Using CLI

This chapter describes how to use the command-line interface of the Adaptive Security Appliance to configure the VPN Client parameters. As with the other chapters, this one focuses on those parameters that you must configure specifically for the VPN Client. The IPsec group uses the IPsec connection parameters to create a tunnel. This chapter focuses only on the parameters related to the VPN. For complete information about configuration using the CLI, see the *Cisco ASA 5500 Series Adaptive Security Appliance Configuration Guide*.

The general considerations are the same for both the CLI and ASDM, in that you must configure the following parameters for the VPN Client:

- Configure the IPsec connection profile.
- · Configure the advanced IPsec features.
- · Configure Client Update.

This chapter includes the following sections.

- Configuring Connection Profiles—Overview, page 3-1
- Configuring Connection Profiles—Specifics, page 3-4
- Configuring Group Policies, page 3-11
- Example: Configuring a Security Appliance for the VPN Client Using CLI, page 3-29

We recommend that you carefully read the chapter "Configuring Connection Profiles, Group Policies, and Users Using CLI" in *Cisco Security Appliance Command Line Configuration Guide* for a complete description of all the parameters you can configure for IPsec connections. That chapter contains complete information on setting up remote users to connect through the IPsec tunnel, and also explains how to use features such as setting up a client banner, firewalls, split tunneling, and so on.

Configuring Connection Profiles—Overview

You configure the parameters in this section using tunnel-group commands. An IPsec connection represents a connection-specific record for IPsec VPN connections. In summary, you first configure connection profiles to set the values for the connection. Then you configure group policies. These set values for users in the aggregate. Then you configure users, which can inherit values from groups and configure certain values on an individual user basis. This chapter describes how and why to configure VPN Client-related parameters for connection profiles and group policies.

To configure the IPsec connection profile, do the following steps:

- Step 1 Configure the IPsec connection profile. You specify a connection-profile name when you add or edit a connection profile. The following considerations apply:
 - For clients that use preshared keys to authenticate, the connection profile name is the same as the group name that an IPsec client passes to the security appliance.
 - Clients that use certificates to authenticate pass this name as part of the certificate, and the security appliance extracts the name from the certificate.
- Step 2 In the Access Interfaces area, enable the appropriate interfaces (which you've already configured) to allow IPsec access.
- Step 3 If necessary, add a new connection profile or edit an existing profile in the Connection Profiles area.

Configuring General Connection Profile Parameters

General parameters are common to all VPN connections. While you must configure all of these parameters (or accept the default values), the following sections concentrate on the ones you must configure for VPN Client connections. The general parameters include the following:

- Connection profile name—You specify a connection-profile name when you add or edit a connection profile. The following considerations apply:
 - For clients that use preshared keys to authenticate, the connection profile name is the same as the group name that an IPsec client passes to the security appliance.
 - Clients that use certificates to authenticate pass this name as part of the certificate, and the security appliance extracts the name from the certificate.
- Connection type—Connection types include IPsec remote access, IPsec LAN-to-LAN, and
 clientless SSL VPN. A connection profile can have only one connection type. For the VPN Client,
 you must configure at least one IPsec remote access connection profile.
- Authentication, Authorization, and Accounting servers—These parameters identify the server groups or lists that the security appliance uses for the following purposes:
 - Authenticating users
 - Obtaining information about services users are authorized to access
 - Storing accounting records

A server group can consist of one or more servers.

- Default group policy for the connection—A group policy is a set of user-oriented attributes. The
 default group policy is the group policy whose attributes the security appliance uses as defaults
 when authenticating or authorizing a tunnel user.
- Client address assignment method—This method includes values for one or more DHCP servers or address pools that the security appliance assigns to clients.
- Override account disabled—This parameter lets you override the "account-disabled" indicator received from a AAA server.
- Password management—This parameter lets you warn a user that the current password is due to
 expire in a specified number of days (the default is 14 days), then offer the user the opportunity to
 change the password.

• Strip group and strip realm—These parameters direct the way the security appliance processes the usernames it receives. They apply only to usernames received in the form user@realm. A realm is an administrative domain appended to a username with the @ delimiter (user@abc).

When you specify the **strip-group** command, the security appliance selects the connection profile for user connections by obtaining the group name from the username presented by the VPN client. The security appliance then sends only the user part of the username for authorization/authentication. Otherwise (if disabled), the security appliance sends the entire username, including the realm.

Strip-realm processing removes the realm from the username when sending the username to the authentication or authorization server. If the command is enabled, the security appliance sends only the user part of the username authorization/authentication. Otherwise, the security appliance sends the entire username.

- Authorization required—This parameter lets you require authorization before a user can connect, or turn off that requirement.
- Authorization DN attributes—This parameter specifies which Distinguished Name attributes to use
 when performing authorization.

IPsec Connection Profile Parameters

IPsec connection profile/tunnel group parameters include the following:

- A client authentication method: preshared keys, certificates, or both.
 - For IKE connections based on preshared keys, this is the alphanumeric key itself (up to 128 characters long), associated with the connection policy.
 - Peer-ID validation requirement—This parameter specifies whether to require validating the identity of the peer using the peer's certificate.
- An extended hybrid authentication method: XAUTH and hybrid XAUTH.

You use the **isakmp ikev1-user-authentication** command to implement hybrid XAUTH authentication when you need to use digital certificates for security appliance authentication and a different, legacy method for remote VPN user authentication, such as RADIUS, TACACS+ or SecurID.

• ISAKMP (IKE) keepalive settings. This feature lets the security appliance monitor the continued presence of a remote peer and report its own presence to that peer. If the peer becomes unresponsive, the security appliance removes the connection. Enabling IKE keepalives prevents hung connections when the IKE peer loses connectivity.

There are various forms of IKE keepalives. For this feature to work, both the security appliance and its remote peer must support a common form. This feature works with the following peers:

- Cisco AnyConnect VPN Client
- Cisco VPN Client (Release 3.0 and above)
- Cisco VPN 3000 Client (Release 2.x)
- Cisco VPN 3002 Hardware Client
- Cisco VPN 3000 Series Concentrators
- Cisco IOS software
- Cisco Secure PIX Firewall

Non-Cisco VPN clients do not support IKE keepalives.

If you are configuring a group of mixed peers, and some of those peers support IKE keepalives and others do not, enable IKE keepalives for the entire group. The feature does not affect the peers that do not support it.

If you disable IKE keepalives, connections with unresponsive peers remain active until they time out, so we recommend that you keep your idle timeout short. To change your idle timeout, see the "Configuring Group Policies" section on page 3-14.

- If you configure authentication using digital certificates, you can specify whether to send the entire certificate chain (which sends the peer the identity certificate and all issuing certificates) or just the issuing certificates (including the root certificate and any subordinate CA certificates).
- You can notify users who are using outdated versions of Windows client software that they need to
 update their client, and you can provide a mechanism for them to get the updated client version. For
 VPN 3002 hardware client users, you can trigger an automatic update. You can configure and change
 the client-update, either for all connection profiles or for particular connection profiles.
- If you configure authentication using digital certificates, you can specify the name of the trustpoint that identifies the certificate to send to the IKE peer.

Configuring Connection Profiles—Specifics

The following sections describe the contents and configuration of connection profiles:

- Default IPsec Remote Access Connection Profile Configuration, page 3-4
- Specifying a Name and Type for the IPsec Remote Access Connection Profile, page 3-5
- Configuring IPsec Remote-Access Connection Profiles, page 3-5

You can modify the default connection profiles, and you can configure a new connection profile as any of the three tunnel-group types. If you don't explicitly configure an attribute in a connection profile, that attribute gets its value from the default connection profile. The default connection-profile type is remote access. The subsequent parameters depend upon your choice of tunnel type. To see the current configured and default configuration of all your connection profiles, including the default connection profile, enter the **show running-config all tunnel-group** command.

Default IPsec Remote Access Connection Profile Configuration

The contents of the default remote-access connection profile are as follows:

```
tunnel-group DefaultRAGroup type remote-access
tunnel-group DefaultRAGroup general-attributes
no address-pool
no ipv6-address-pool
authentication-server-group LOCAL
 accounting-server-group RADIUS
default-group-policy DfltGrpPolicy
no dhcp-server
no strip-realm
no password-management
no override-account-disable
no strip-group
authorization-dn-attributes CN OU
tunnel-group DefaultRAGroup webvpn-attributes
hic-fail-group-policy DfltGrpPolicy
 customization DfltCustomization
 authentication aaa
```

```
no override-svc-download
no radius-reject-message
dns-group DefaultDNS
tunnel-group DefaultRAGroup ipsec-attributes
no pre-shared-key
peer-id-validate req
no chain
no trust-point
isakmp keepalive threshold 1500 retry 2
no radius-sdi-xauth
isakmp ikev1-user-authentication xauth
tunnel-group DefaultRAGroup ppp-attributes
no authentication pap
authentication chap
authentication ms-chap-v1
no authentication ms-chap-v2
no authentication eap-proxy
```

Configuring IPsec Tunnel-Group General Attributes

The general attributes are common across more than one connection-profile type. IPsec remote access and clientless SSL VPN tunnels share most of the same general attributes. IPsec LAN-to-LAN tunnels use a subset. Refer to the *Cisco Security Appliance Command Reference* for complete descriptions of all commands. The following sections describe, in order, how to configure IPsec remote-access connection profiles.

Configuring IPsec Remote-Access Connection Profiles

Use an IPsec remote-access connection profile when setting up a connection between a remote client and a central-site security appliance, using a hardware or software client. To configure an IPsec remote-access connection profile, first configure the tunnel-group general attributes, then the IPsec remote-access attributes. An IPsec Remote Access VPN connection profile applies only to remote-access IPsec client connections. To configure an IPsec remote-access connection profile, see the following sections:

- Specifying a Name and Type for the IPsec Remote Access Connection Profile, page 3-5.
- Configuring IPsec Remote-Access Connection Profile General Attributes, page 3-6.
- Configuring IPsec Remote-Access Connection Profile IPsec Attributes, page 3-7.

Specifying a Name and Type for the IPsec Remote Access Connection Profile

Create the connection profile, specifying its name and type, by entering the **tunnel-group** command. For an IPsec remote-access tunnel, the type is **remote-access**

```
hostname(config)# tunnel_group_name type remote-access
hostname(config)#
```

For example, to create an IPsec remote-access connection profile named TunnelGroup1, enter the following command:

```
hostname(config) # tunnel-group TunnelGroup1 type remote-access
hostname(config) #
```

Configuring IPsec Remote-Access Connection Profile General Attributes

In general, you can accept the default values for all of the general attributes, although you might have a particular set of parameters that you want to change. To configure or change the connection profile general attributes, specify the parameters in the following steps.

Step 1 To configure the general attributes, enter the **tunnel-group general-attributes** command, which enters tunnel-group general-attributes configuration mode. The prompt changes to indicate the change in mode.

```
hostname(config)# tunnel-group tunnel_group_name general-attributes
hostname(config-tunnel-general)#
```

Step 2 Specify the name of the authentication-server group, if any, to use. If you want to use the LOCAL database for authentication if the specified server group fails, append the keyword **LOCAL**:

```
hostname(config-tunnel-general)# authentication-server-group [(interface_name)] groupname [LOCAL] hostname(config-tunnel-general)#
```

The name of the authentication server group can be up to 16 characters long.

You can optionally configure interface-specific authentication by including the name of an interface after the group name. The interface name, which specifies where the IPsec tunnel terminates, must be enclosed in parentheses. The following command configures interface-specific authentication for the interface named test using the server named servergroup1 for authentication:

```
hostname(config-tunnel-general)# authentication-server-group (test) servergroup1
hostname(config-tunnel-general)#
```

Step 3 Specify the name of the authorization-server group, if any, to use. When you configure this value, users must exist in the authorization database to connect:

```
hostname(config-tunnel-general)# authorization-server-group groupname
hostname(config-tunnel-general)#
```

The name of the authorization server group can be up to 16 characters long. For example, the following command specifies the use of the authorization-server group FinGroup:

```
hostname(config-tunnel-general)# authorization-server-group FinGroup
hostname(config-tunnel-general)#
```

Step 4 Specify the name of the accounting-server group, if any, to use:

```
hostname(config-tunnel-general)# accounting-server-group groupname
hostname(config-tunnel-general)#
```

The name of the accounting server group can be up to 16 characters long. For example, the following command specifies the use of the accounting-server group named comptroller:

```
hostname(config-tunnel-general)# accounting-server-group comptroller
hostname(config-tunnel-general)#
```

Step 5 Specify the name of the default group policy:

```
hostname(config-tunnel-general)# default-group-policy policyname
hostname(config-tunnel-general)#
```

The name of the group policy can be up to 64 characters long. The following example sets DfltGrpPolicy as the name of the default group policy:

```
hostname(config-tunnel-general)# default-group-policy DfltGrpPolicy
hostname(config-tunnel-general)#
```

Step 6 Specify the names or IP addresses of the DHCP server (up to 10 servers), and the names of the DHCP address pools (up to 6 pools). The defaults are no DHCP server and no address pool.

```
hostname(config-tunnel-general)# dhcp-server server1 [...server10]
hostname(config-tunnel-general)# address-pool [(interface name)] address_pool1
[...address_pool6]
hostname(config-tunnel-general)#
```



Note

If you specify an interface name, you must enclosed it within parentheses.

You configure address pools with the **ip local pool** command in global configuration mode.

Step 7 Specify the attribute or attributes to use in deriving a name for an authorization query from a certificate.

This attribute specifies what part of the subject DN field to use as the username for authorization:

```
hostname(config-tunnel-general)# username-from-certificate {primary-attribute [secondary-attribute] | use-entire-name}
```

For example, the following command specifies the use of the CN attribute as the username for authorization:

```
hostname(config-tunnel-general)# username-from-certificate CN
hostname(config-tunnel-general)#
```

The authorization-dn-attributes are C (Country), CN (Common Name), DNQ (DN qualifier), EA (E-mail Address), GENQ (Generational qualifier), GN (Given Name), I (Initials), L (Locality), N (Name), O (Organization), OU (Organizational Unit), SER (Serial Number), SN (Surname), SP (State/Province), T (Title), UID (User ID), and UPN (User Principal Name).

Configuring IPsec Remote-Access Connection Profile IPsec Attributes

To configure the IPsec attributes for a remote-access connection profile, do the following steps. The following description assumes that you have already created the IPsec remote-access connection profile.

If you have a LAN-to-LAN configuration using IKE main mode, make sure that the two peers have the same IKE keepalive configuration. Both peers must have IKE keepalives enabled or both peers must have it disabled.



Note

To reduce connectivity costs, disable IKE keepalives if this group includes any clients connecting via ISDN lines. ISDN connections normally disconnect if idle, but the IKE keepalive mechanism prevents connections from idling and therefore from disconnecting.

If you do disable IKE keepalives, the client disconnects only when either its IKE or IPsec keys expire. Failed traffic does not disconnect the tunnel with the Peer Timeout Profile values as it does when IKE keepalives are enabled.

To configure the IPsec attributes for an IPsec connection profile, do the following steps:

Step 1 To specify the attributes of an IPsec remote-access connection profile, enter tunnel-group ipsec-attributes mode by entering the following command. The prompt changes to indicate the mode change:

hostname(config)# tunnel-group tunnel-group-name ipsec-attributes

```
hostname(config-tunnel-ipsec)#
```

This command enters tunnel-group ipsec-attributes configuration mode, in which you configure the remote-access tunnel-group IPsec attributes.

For example, the following command designates that the tunnel-group ipsec-attributes mode commands that follow pertain to the connection profile named TG1. Notice that the prompt changes to indicate that you are now in tunnel-group ipsec-attributes mode:

```
hostname(config)# tunnel-group TG1 type remote-access
hostname(config)# tunnel-group TG1 ipsec-attributes
hostname(config-tunnel-ipsec)#
```

Step 2 Specify the preshared key to support IKE connections based on preshared keys. For example, the following command specifies the preshared key xyzx to support IKE connections for an IPsec remote access connection profile:

```
hostname(config-tunnel-ipsec)# pre-shared-key xyzx
hostname(config-tunnel-ipsec)#
```

Step 3 Specify whether to validate the identity of the peer using the peer's certificate:

```
hostname(config-tunnel-ipsec)# peer-id-validate option
hostname(config-tunnel-ipsec)#
```

The available options are **req** (required), **cert** (if supported by certificate), and **nocheck** (do not check). The default is **req**.

For example, the following command specifies that peer-id validation is required:

```
hostname(config-tunnel-ipsec)# peer-id-validate req
hostname(config-tunnel-ipsec)#
```

Step 4 Specify whether to enable sending of a certificate chain. The following command includes the root certificate and any subordinate CA certificates in the transmission:

```
hostname(config-tunnel-ipsec)# chain
hostname(config-tunnel-ipsec)#
```

This attribute applies to all IPsec tunnel-group types.

Step 5 Specify the name of a trustpoint that identifies the certificate to be sent to the IKE peer:

```
hostname(config-tunnel-ipsec)# trust-point trust-point-name
hostname(config-tunnel-ipsec)#
```

The following command specifies mytrustpoint as the name of the certificate to be sent to the IKE peer:

```
hostname(config-ipsec)# trust-point mytrustpoint
```

Step 6 Specify the ISAKMP (IKE) keepalive threshold and the number of retries allowed.

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold <number> retry <number> hostname(config-tunnel-ipsec)#
```

The **threshold** parameter specifies the number of seconds (10 through 3600) that the peer is allowed to idle before beginning keepalive monitoring. The **retry** parameter is the interval (2 through 10 seconds) between retries after a keepalive response has not been received. IKE keepalives are enabled by default. To disable IKE keepalives, enter the **no** form of the **isakmp** command.

For example, the following command sets the IKE keepalive threshold value to 15 seconds and sets the retry interval to 10 seconds:

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10
hostname(config-tunnel-ipsec)#
```

The default value for the **threshold** parameter is 300 for remote-access and 10 for LAN-to-LAN, and the default value for the retry parameter is 2.

To specify that the central site ("head end") should never initiate ISAKMP monitoring, enter the following command:

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold infinite
hostname(config-tunnel-ipsec)#
```

Step 7 Specify the ISAKMP hybrid authentication method, XAUTH or hybrid XAUTH.

You use **isakmp ikev1-user-authentication** command to implement hybrid XAUTH authentication when you need to use digital certificates for security appliance authentication and a different, legacy method for remote VPN user authentication, such as RADIUS, TACACS+ or SecurID. Hybrid XAUTH breaks phase 1 of IKE down into the following two steps, together called hybrid authentication:

- **a.** The security appliance authenticates to the remote VPN user with standard public key techniques. This establishes an IKE security association that is unidirectionally authenticated.
- b. An XAUTH exchange then authenticates the remote VPN user. This extended authentication can use one of the supported legacy authentication methods.



Before the authentication type can be set to hybrid, you must configure the authentication server, create a preshared key, and configure a trustpoint.

You can use the **isakmp ikev1-user-authentication** command with the optional **interface** parameter to specify a particular interface. When you omit the **interface** parameter, the command applies to all the interfaces and serves as a back-up when the per-interface command is not specified. When there are two **isakmp ikev1-user-authentication** commands specified for a connection profile, and one uses the **interface** parameter and one does not, the one specifying the interface takes precedence for that particular interface.

For example, the following commands enable hybrid XAUTH on the inside interface for a connection profile called example-group:

```
hostname(config)# tunnel-group example-group type remote-access
hostname(config)# tunnel-group example-group ipsec-attributes
hostname(config-tunnel-ipsec)# isakmp ikev1-user-authentication (inside) hybrid
hostname(config-tunnel-ipsec)#
```

Configuring Client Software Update Using ASDM

The optional client update feature ensures acceptable Client revision levels. This feature lets administrators at a central location automatically notify VPN client users that it is time to update the VPN client software and the VPN 3002 hardware client image.

Remote users might be using outdated VPN software or hardware client versions. You can use the client-update feature to enable updating client revisions; specify the types and revision numbers of clients to which the update applies; provide a URL or IP address from which to get the update; and, in the case of Windows clients, optionally notify users that they should update their VPN client version. For Windows clients, you can provide a mechanism for users to accomplish that update. For VPN 3002 hardware client users, the update occurs automatically, with no notification. This feature applies only to the IPsec remote-access tunnel-group type.

If the client is already running a software version that is at least as high as those included on the list of revision numbers, it does not need to update its software. If the client is not running a software version on the list (or a higher version), it should update.

The VPN Client commands list the client type, VPN Client revisions, and image URL for each client VPN software package installed. For each client type, you can specify the acceptable client software revisions and the URL or IP address from which to download software upgrades, if necessary. The client update mechanism (described in detail under the Client Update window) uses this information to determine whether the software each VPN client is running is at an appropriate revision level and, if appropriate, to provide a notification message and an update mechanism to clients that are running outdated software. Specify the following fields to configure client update.

To configure the VPN Client software update feature, perform the following steps:

Step 1 Enable client update

client-update enable

This command enables client update, both globally and for specific tunnel groups. You must enable client update before you can send a client update notification to Windows, MAC OS X, and Linux VPN clients, or initiate an automatic update to hardware clients.

Step 2 Specify the type of client update that you want to configure. Use the client-update command:

client-update type client-type url image-url revisions

where:

- client-type lists the clients to upgrade: software or hardware, and for Windows software clients, all Windows or a subset. Possible values are:
 - Win9X—Includes Windows 95, Windows 98 and Windows ME platforms.
 - WinNT—Includes Windows NT 4.0, Windows 2000, Windows XP, and Windows Vista platforms.
 - Windows—Includes all Windows based platforms.
 - linux-Linux client.
 - Mac OS X—Mac OS X client.
 - solaris—Solaris client
 - vpn3002—VPN3002 Hardware client.

If you specify **windows**, do not specify Windows versions individually. The secure gateway sends a separate notification message for each entry in a client-update list; therefore, your client-update entries must not overlap. For example, the value "Windows" includes all Windows platforms, and the value "WinNT" includes Windows Vista, Windows XP, Windows 2000, and Windows NT 4.0, so you would not specify both "Windows" and "Windows NT." To find out the client types and version information, click the lock icon at the top left corner of the Cisco Systems VPN Client main window and choose "About VPN Client".

The hardware client gets updated with a release of the ASA 5505 software or of the VPN 3002 hardware client.



If the client update feature has already been configured to support all Windows clients, you must remove that specification before specifying individual Windows client types.

- image-url—Specifies the URL or IP address from which to download the software image. This URL must point to a file appropriate for this client. For Windows, MAC OS X, and Linux-based clients, the URL must be in the form: http:// or https://. For hardware clients, the URL must be in the form tftp://.
 - For Windows, MAC OS X, and Linux-based VPN clients: To activate the Launch button on the VPN Client Notification, the URL must include the protocol HTTP or HTTPS and the server address of the site that contains the update. The format of the URL is: http(s)://server_address:port/directory/filename. The server address can be either an IP address or a hostname if you have configured a DNS server. For example:

```
http://10.10.99.70/vpnclient-win-4.6.Rel-k9.exe
```

The directory is optional. You need the port number only if you use ports other than 80 for HTTP or 443 for HTTPS.

 For the hardware client: The format of the URL is tftp://server_address/directory/filename. The server address can be either an IP address or a hostname if you have configured a DNS server.
 For example:

```
tftp://10.1.1.1/vpn3002-4.1.Rel-k9.bin
```

- revisions—Specifies a comma-separated list of software image revisions appropriate for this client.
 If the user's client revision number matches or is higher than one of the specified revision numbers, there is no need to update the client, and, for Windows-based clients, the user does not receive an update notification. The following caveats apply:
 - The revision list must include the software version for this update.
 - Your entries must match exactly those on the URL for the VPN client, or the TFTP server for the hardware client.
 - The TFTP server for distributing the hardware client image must be a robust TFTP server.
 - A VPN client user must download an appropriate software version from the listed URL.
 - The VPN 3002 hardware client software is automatically updated via TFTP, with no notification to the user.

Configuring Group Policies

A group policy is a set of user-oriented attribute/value pairs for IPsec connections that are stored either internally (locally) on the device or externally on a RADIUS server. The connection profile uses a group policy that sets terms for user connections after the tunnel is established. Group policies let you apply whole sets of attributes to a user or a group of users, rather than having to specify each attribute individually for each user.

Enter the **group-policy** commands in global configuration mode to assign a group policy to users or to modify a group policy for specific users.

The security appliance includes a default group policy. In addition to the default group policy, which you can modify but not delete, you can create one or more group policies specific to your environment.

You can configure internal and external group policies. Internal groups are configured on the security appliance's internal database. External groups are configured on an external authentication server, such as RADIUS. Group policies include the following attributes:

- Identity
- · Server definitions
- · Client firewall settings
- Tunneling protocols
- · IPsec settings
- · Hardware client settings
- Filters
- Client configuration settings
- Connection settings

Only a subset of group-policy parameters pertain specifically to the VPN Client. This section focuses only on the commands you use to configure those parameters on the security appliance. For a complete description of configuring group policies for the security appliance, see *Cisco Security Appliance Command Line Configuration Guide*.

Default Group Policy

The security appliance supplies a default group policy. You can modify this default group policy, but you cannot delete it. A default group policy, named DfltGrpPolicy, always exists on the security appliance, but this default group policy does not take effect unless you configure the security appliance to use it. When you configure other group policies, any attribute that you do not explicitly specify takes its value from the default group policy. To view the default group policy, enter the following command:

```
hostname(config) # show running-config all group-policy DfltGrpPolicy
hostname(confiq) #
```

To configure the default group policy, enter the following command:

```
hostname(config)# group-policy DfltGrpPolicy internal
hostname(config)#
```



The default group policy is always internal. Despite the fact that the command syntax is hostname(config)# group-policy DfltGrpPolicy {internal | external}, you cannot change its type to external.

To change any of the attributes of the default group policy, use the **group-policy attributes** command to enter attributes mode, then specify the commands to change whatever attributes that you want to modify:

hostname(config)# group-policy DfltGrpPolicy attributes



The attributes mode applies only to internal group policies.

The default group policy, DfltGrpPolicy, that the security appliance provides is as follows:

```
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
banner none
 wins-server none
 dns-server none
 dhcp-network-scope none
 vpn-access-hours none
 vpn-simultaneous-logins 3
 vpn-idle-timeout 30
 vpn-session-timeout none
 vpn-filter none
 ipv6-vpn-filter none
 vpn-tunnel-protocol IPSec svc webvpn
password-storage disable
 ip-comp disable
 re-xauth disable
 group-lock none
 pfs disable
 ipsec-udp disable
 ipsec-udp-port 10000
 split-tunnel-policy tunnelall
 split-tunnel-network-list none
 default-domain none
 split-dns none
 intercept-dhcp 255.255.255.255 disable
 secure-unit-authentication disable
 user-authentication disable
 user-authentication-idle-timeout 30
 ip-phone-bypass disable
 leap-bypass disable
nem disable
backup-servers keep-client-config
msie-proxy server none
msie-proxy method no-modify
msie-proxy except-list none
msie-proxy local-bypass disable
msie-proxy pac-url none
 vlan none
nac-settings none
 address-pools none
 ipv6-address-pools none
 smartcard-removal-disconnect enable
 client-firewall none
 client-access-rule none
 webvpn
 url-list value Engineering
  filter none
  homepage none
 html-content-filter none
  port-forward name Application Access
  port-forward disable
  mapi disable
  http-proxy disable
  sso-server none
  svc dtls enable
  svc mtu 1406
  svc keep-installer installed
  svc keepalive 20
  svc rekey time none
  svc rekey method none
  svc dpd-interval client 30
  svc dpd-interval gateway 30
  svc compression deflate
  svc modules none
```

```
svc profiles none
  svc ask none
 ike-retry-timeout 10
 ike-retry-count 3
  customization none
  keep-alive-ignore 4
 http-comp gzip
  download-max-size 2147483647
 upload-max-size 2147483647
  post-max-size 2147483647
 user-storage none
  storage-objects value cookies, credentials
 storage-key none
 hidden-shares none
  smart-tunnel disable
  activex-relay enable
 unix-auth-uid 65534
 unix-auth-gid 65534
  file-entry enable
  file-browsing enable
 url-entry enable
 deny-message value Login was successful, but because certain criteria have not been met
or due to some specific group policy, you do not have permission to use any of the VPN
features. Contact your IT administrator for more information
hostname(config)#
```

You can modify the default group policy, and you can also create one or more group policies specific to your environment.

Configuring Group Policies

A group policy can apply to any kind of tunnel. In each case, if you do not explicitly define a parameter, the group takes the value from the default group policy. To configure a group policy, follow the steps in the subsequent sections.

Configuring an Internal Group Policy

To configure an internal group policy, specify a name and type for the group policy:

```
hostname(config)# group-policy group_policy_name type
hostname(config)#
```

For example, the following command creates the internal group policy named GroupPolicy1:

```
hostname(config)# group-policy GroupPolicy1 internal
hostname(config)#
```

The default type is internal.

You can initialize the attributes of an internal group policy to the values of a preexisting group policy by appending the keyword **from** and specifying the name of the existing policy:

```
hostname(config) # group-policy group_policy_name internal from group_policy_name
hostname(config-group-policy) #
hostname(config-group-policy) #
```

Configuring Group Policy Attributes

For internal group policies, you can specify particular attribute values. To begin, enter group-policy attributes mode, by entering the **group-policy attributes** command in global configuration mode.

```
hostname(config)# group-policy name attributes
hostname(config-group-policy)#
```

The prompt changes to indicate the mode change. The group-policy-attributes mode lets you configure attribute-value pairs for a specified group policy. In group-policy-attributes mode, explicitly configure the attribute-value pairs that you do not want to inherit from the default group. The commands to do this are described in the following sections.

Configuring VPN-Specific Attributes

Follow the steps in this section to set the VPN attribute values. The VPN attributes control the access hours, the number of simultaneous logins allowed, the timeouts, the egress VLAN or ACL to apply to VPN sessions, and the tunnel protocol:

Step 1 Set the VPN access hours. To do this, you associate a group policy with a configured time-range policy, using the **vpn-access-hours** command in group-policy configuration mode.

```
hostname(config-group-policy)# vpn-access-hours value {time-range | none}
```

A group policy can inherit a time-range value from a default or specified group policy. To prevent this inheritance, enter the **none** keyword instead of the name of a time-range in this command. This keyword sets VPN access hours to a null value, which allows no time-range policy.

The time-range variable is the name of a set of access hours defined in global configuration mode using the **time-range** command. The following example shows how to associate the group policy named FirstGroup with a time-range policy called 824:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-access-hours value 824
```

Step 2 Specify the number of simultaneous logins allowed for any user, using the **vpn-simultaneous-logins** command in group-policy configuration mode.

```
hostname(config-group-policy)# vpn-simultaneous-logins integer
```

The default value is 3. The range is an integer in the range 0 through 2147483647. A group policy can inherit this value from another group policy. Enter 0 to disable login and prevent user access. The following example shows how to allow a maximum of 4 simultaneous logins for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-simultaneous-logins 4
hostname(config-group-policy)#
```



While the maximum limit for the number of simultaneous logins is very large, allowing several simultaneous logins could compromise security and affect performance.

Stale AnyConnect, IPsec Client, or Clientless sessions (sessions that are terminated abnormally) might remain in the session database, even though a "new" session has been established with the same username.

If the value of vpn-simultaneous-logins is 1, and the same user logs in again after an abnormal termination, then the stale session is removed from the database and the new session is established. If, however, the existing session is still an active connection and the same user logs in again, perhaps from another PC, the first session is logged off and removed from the database, and the new session is established.

If the number of simultaneous logins is a value greater than 1, then, when you have reached that maximum number and try to log in again, the session with the longest idle time is logged off. If all current sessions have been idle an equally long time, then the oldest session is logged off. This action frees up a session and allows the new login.

Step 3 Configure the user timeout period by entering the **vpn-idle-timeout** command in group-policy configuration mode or in username configuration mode:

```
hostname(config-group-policy)# vpn-idle-timeout {minutes | none}
hostname(config-group-policy)#
```

The minimum time is 1 minute, and the maximum time is 35791394 minutes. The default is 30 minutes. If there is no communication activity on the connection in this period, the security appliance terminates the connection.

A group policy can inherit this value from another group policy. To prevent inheriting a value, enter the **none** keyword instead of specifying a number of minutes with this command. The **none** keyword specifies that this connection uses the global WebVPN idle timeout period specified in the global WebVPN **default-idle-timeout** command. It sets the idle timeout to a null value, thereby disallowing an idle timeout.

The following example shows how to set a VPN idle timeout of 15 minutes for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-idle-timeout 15
hostname(config-group-policy)#
```

Step 4 Configure a maximum amount of time for VPN connections, using the **vpn-session-timeout** command in group-policy configuration mode or in username configuration mode.

```
hostname(config-group-policy)# vpn-session-timeout {minutes | none}
hostname(config-group-policy)#
```

The minimum time is 1 minute, and the maximum time is 35791394 minutes. There is no default value. At the end of this period of time, the security appliance terminates the connection.

A group policy can inherit this value from another group policy. To prevent inheriting a value, enter the **none** keyword instead of specifying a number of minutes with this command. Specifying the **none** keyword permits an unlimited session timeout period and sets session timeout with a null value, which disallows a session timeout.

The following example shows how to set a VPN session timeout of 180 minutes for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-session-timeout 180
hostname(config-group-policy)#
```

Step 5 Specify the VPN connection policy for this group policy. For an IPsec connection, specify **ipsec**.

```
hostname(config-group-policy)# vpn-tunnel-protocol {webvpn | ipsec | 12tp-ipsec}
hostname(config-group-policy)#
```

The default is ipsec. To remove the attribute from the running configuration, enter the **no** form of this command.

```
hostname(config-group-policy) # no vpn-tunnel-protocol [webvpn | ipsec | 12tp-ipsec]
hostname(config-group-policy) #
```

The parameter values for this command follow:

- **ipsec**—Negotiates an IPsec tunnel between two peers (a remote access client or another secure gateway). Creates security associations that govern authentication, encryption, encapsulation, and key management.
- **webvpn**—Provides VPN services to remote users via an HTTPS-enabled web browser, and does not require a client.
- 12tp-ipsec—Negotiates an IPsec tunnel for an L2TP connection

Enter this command to configure one or more tunneling modes. You must configure at least one tunneling mode for users to connect over a VPN tunnel.

The following example shows how to configure the IPsec tunneling mode for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-tunnel-protocol ipsec
hostname(config-group-policy)#
```

Configuring Security Attributes

The attributes in this section specify certain security settings for the group. We recommend accepting the default values for these parameters unless you have a good reason for changing them:

Step 1 Specify whether to let users store their login passwords on the client system, using the password-storage command with the enable keyword in group-policy configuration mode. To disable password storage, use the password-storage command with the disable keyword.

```
hostname(config-group-policy) # password-storage {enable | disable}
hostname(config-group-policy) #
```

For security reasons, password storage is disabled by default. Enable password storage only on systems that you know to be in secure sites.

To remove the password-storage attribute from the running configuration, enter the **no** form of this command:

```
hostname(config-group-policy) # no password-storage
hostname(config-group-policy) #
```

Specifying the **no** form enables inheritance of a value for password-storage from another group policy.

This command does not apply to interactive hardware client authentication or individual user authentication for hardware clients.

The following example shows how to enable password storage for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# password-storage enable
hostname(config-group-policy)#
```

Step 2 Specify whether to enable IP compression, which is disabled by default.

```
hostname(config-group-policy)# ip-comp {enable | disable}
hostname(config-group-policy)#
```

To enable LZS IP compression, enter the **ip-comp** command with the **enable** keyword in group-policy configuration mode. To disable IP compression, enter the **ip-comp** command with the **disable** keyword.

To remove the **ip-comp** attribute from the running configuration, enter the **no** form of this command. This enables inheritance of a value from another group policy.

```
hostname(config-group-policy)# no ip-comp
hostname(config-group-policy)#
```

Enabling data compression might speed up data transmission rates for remote dial-in users connecting with modems.



Data compression increases the memory requirement and CPU usage for each user session and consequently decreases the overall throughput of the security appliance. For this reason, we recommend that you enable data compression only for remote users connecting with a modem. Design a group policy specific to modem users, and enable compression only for them.

Step 3 Specify whether to require that users reauthenticate on IKE rekey by using the **re-xauth** command with the **enable** keyword in group-policy configuration mode. If you enable reauthentication on IKE rekey, the security appliance prompts the user to enter a username and password during initial Phase 1 IKE negotiation and also prompts for user authentication whenever an IKE rekey occurs. Reauthentication provides additional security.

If the configured rekey interval is very short, users might find the repeated authorization requests inconvenient. To avoid repeated authorization requests, disable reauthentication. To check the configured rekey interval, in monitoring mode, enter the **show crypto ipsec sa** command to view the security association lifetime in seconds and lifetime in kilobytes of data. To disable user reauthentication on IKE rekey, enter the **disable** keyword. Reauthentication on IKE rekey is disabled by default.

```
hostname(config-group-policy)# re-xauth {enable | disable}
hostname(config-group-policy)#
```

To enable inheritance of a value for reauthentication on IKE rekey from another group policy, remove the re-xauth attribute from the running configuration by entering the **no** form of this command.

```
hostname(config-group-policy)# no re-xauth
hostname(config-group-policy)#
```



Reauthentication fails if there is no user at the other end of the connection.

Step 4 Specify whether to restrict remote users to access only through the connection profile, using the **group-lock** command in group-policy configuration mode.

```
hostname(config-group-policy)# group-lock {value tunnel-grp-name | none}
hostname(config-group-policy)# no group-lock
hostname(config-group-policy)#
```

The *tunnel-grp-name* variable specifies the name of an existing connection profile that the security appliance requires for the user to connect. Group-lock restricts users by checking if the group configured in the VPN client is the same as the connection profile to which the user is assigned. If it is not, the security appliance prevents the user from connecting. If you do not configure group-lock, the security appliance authenticates users without regard to the assigned group. Group locking is disabled by default.

To remove the **group-lock** attribute from the running configuration, enter the **no** form of this command. This option allows inheritance of a value from another group policy.

To disable group-lock, enter the **group-lock** command with the **none** keyword. The none keyword sets group-lock to a null value, thereby allowing no group-lock restriction. It also prevents inheriting a group-lock value from a default or specified group policy

Step 5 Specify whether to enable perfect forward secrecy. In IPsec negotiations, perfect forward secrecy ensures that each new cryptographic key is unrelated to any previous key. A group policy can inherit a value for perfect forward secrecy from another group policy. Perfect forward secrecy is disabled by default. To enable perfect forward secrecy, use the **pfs** command with the **enable** keyword in group-policy configuration mode.

```
hostname(config-group-policy)# pfs {enable | disable}
hostname(config-group-policy)#
```

To disable perfect forward secrecy, enter the **pfs** command with the **disable** keyword.

To remove the perfect forward secrecy attribute from the running configuration and prevent inheriting a value, enter the **no** form of this command.

```
hostname(config-group-policy) # no pfs
hostname(config-group-policy) #
```

Configuring the Banner Message

Specify the banner, or welcome message, if any, that you want to display. The default is no banner. The message that you specify is displayed on remote clients when they connect. To specify a banner, enter the **banner** command in group-policy configuration mode. The banner text can be up to 510 characters long. Enter the "\n" sequence to insert a carriage return.



A carriage-return/line-feed included in the banner counts as two characters.

To delete a banner, enter the **no** form of this command. Be aware that using the **no** version of the command deletes all banners for the group policy.

A group policy can inherit this value from another group policy. To prevent inheriting a value, enter the **none** keyword instead of specifying a value for the banner string, as follows:

```
hostname(config-group-policy)# banner {value banner_string | none}
```

The following example shows how to create a banner for the group policy named FirstGroup:

```
hostname(config) # group-policy FirstGroup attributes
hostname(config-group-policy) # banner value Welcome to Cisco Systems 7.0.
```

Configuring IPsec-UDP Attributes

IPsec over UDP, sometimes called IPsec through NAT, lets a Cisco VPN client or hardware client connect via UDP to a security appliance that is running NAT. It is disabled by default. IPsec over UDP is proprietary; it applies only to remote-access connections, and it requires mode configuration. The security appliance exchanges configuration parameters with the client while negotiating SAs. Using IPsec over UDP may slightly degrade system performance.

To enable IPsec over UDP, configure the **ipsec-udp** command with the **enable** keyword in group-policy configuration mode, as follows:

```
hostname(config-group-policy) # ipsec-udp {enable | disable}
```

```
hostname(config-group-policy)# no ipsec-udp
```

To use IPsec over UDP, you must also configure the **ipsec-udp-port** command, as described below.

To disable IPsec over UDP, enter the **disable** keyword. To remove the IPsec over UDP attribute from the running configuration, enter the **no** form of this command. This enables inheritance of a value for IPsec over UDP from another group policy.

The Cisco VPN client must also be configured to use IPsec over UDP (it is configured to use it by default). The VPN 3002 requires no configuration to use IPsec over UDP.

The following example shows how to set IPsec over UDP for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes hostname(config-group-policy)# ipsec-udp enable
```

If you enabled IPsec over UDP, you must also configure the **ipsec-udp-port** command in group-policy configuration mode. This command sets a UDP port number for IPsec over UDP. In IPsec negotiations, the security appliance listens on the configured port and forwards UDP traffic for that port even if other filter rules drop UDP traffic. The port numbers can range from 4001 through 49151. The default port value is 10000.

To disable the UDP port, enter the **no** form of this command. This enables inheritance of a value for the IPsec over UDP port from another group policy.

```
hostname(config-group-policy)# ipsec-udp-port port
```

The following example shows how to set an IPsec UDP port to port 4025 for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipsec-udp-port 4025
```

Configuring Split-Tunneling Attributes

Split tunneling lets a remote-access IPsec client conditionally direct packets over an IPsec tunnel in encrypted form or to a network interface in clear text form. With split tunneling enabled, packets not bound for destinations on the other side of the IPsec tunnel do not have to be encrypted, sent across the tunnel, decrypted, and then routed to a final destination. This command applies this split tunneling policy to a specific network.

Setting the Split-Tunneling Policy

Set the rules for tunneling traffic by specifying the split-tunneling policy:

```
hostname(config-group-policy)# split-tunnel-policy {tunnelall | tunnelspecified |
excludespecified}
hostname(config-group-policy)# no split-tunnel-policy
```

The default is to tunnel all traffic. To set a split tunneling policy, enter the **split-tunnel-policy** command in group-policy configuration mode. To remove the **split-tunnel-policy** attribute from the running configuration, enter the **no** form of this command. This enables inheritance of a value for split tunneling from another group policy.

The **excludespecified** keyword defines a list of networks to which traffic goes in the clear. This feature is useful for remote users who want to access devices on their local network, such as printers, while they are connected to the corporate network through a tunnel. This option applies only to the Cisco VPN client. Configure the ACL is one of the following three methods:

- 0.0.0.0/0.0.0 (Any)—The client learns the local network from the local adapter and routes the
 local network traffic through the local adapter while sending all other traffic through the VPN
 tunnel.
- 0.0.0.0/255.255.255.255 (host 0.0.0.0)—The client routes the local network traffic through the local adapter and all other traffic through the VPN tunnel.
- 10.0.0.0/0.255.255.255—the client routes traffic for the 10.0.0.0/8 network through the local adapter and all other traffic through the VPN tunnel.

The **tunnelall** keyword specifies that no traffic goes in the clear or to any other destination than the security appliance. This, in effect, disables split tunneling. Remote users reach Internet networks through the corporate network and do not have access to local networks. This is the default option.

The **tunnelspecified** keyword tunnels all traffic from or to the specified networks. This option enables split tunneling. It lets you create a network list of addresses to tunnel. Data to all other addresses travels in the clear and is routed by the remote user's Internet service provider.



Split tunneling is primarily a traffic management feature, not a security feature. For optimum security, we recommend that you do not enable split tunneling.

The following example shows how to set a split tunneling policy of tunneling only specified networks for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-policy tunnelspecified
```

Creating a Network List for Split-Tunneling

Create a network list for split tunneling using the **split-tunnel-network-list** command in group-policy configuration mode.

```
hostname(config-group-policy) # split-tunnel-network-list {value access-list_name | none} hostname(config-group-policy) # no split-tunnel-network-list value [access-list name]
```

Split tunneling network lists distinguish networks that require traffic to travel across the tunnel from those that do not require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, which is an ACL that consists of a list of addresses on the private network. Only standard-type ACLs are allowed.

The **value** access-list name parameter identifies an access list that enumerates the networks to tunnel or not tunnel.

The **none** keyword indicates that there is no network list for split tunneling; the security appliance tunnels all traffic. Specifying the **none** keyword sets a split tunneling network list with a null value, thereby disallowing split tunneling. It also prevents inheriting a default split tunneling network list from a default or specified group policy.

To delete a network list, enter the **no** form of this command. To delete all split tunneling network lists, enter the **no split-tunnel-network-list** command without arguments. This command deletes all configured network lists, including a null list if you created one by entering the **none** keyword.

When there are no split tunneling network lists, users inherit any network lists that exist in the default or specified group policy. To prevent users from inheriting such network lists, enter the **split-tunnel-network-list none** command.

The following example shows how to set a network list called FirstList for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-network-list FirstList
```

Configuring Domain Attributes for Tunneling

You can specify a default domain name for tunneled packets or a list of domains to be resolved through the split tunnel. The following sections describe how to set these domains.

Defining a Default Domain Name for Tunneled Packets

The security appliance passes the default domain name to the IPsec client to append to DNS queries that omit the domain field. When there are no default domain names, users inherit the default domain name in the default group policy. To specify the default domain name for users of the group policy, enter the **default-domain** command in group-policy configuration mode. To delete a domain name, enter the **no** form of this command.

```
hostname(config-group-policy)# default-domain {value domain-name | none} hostname(config-group-policy)# no default-domain [domain-name]
```

The **value** *domain-name* parameter identifies the default domain name for the group. To specify that there is no default domain name, enter the **none** keyword. This command sets a default domain name with a null value, which disallows a default domain name and prevents inheriting a default domain name from a default or specified group policy.

To delete all default domain names, enter the **no default-domain** command without arguments. This command deletes all configured default domain names, including a null list if you created one by entering the **default-domain** command with the **none** keyword. The **no** form allows inheriting a domain name.

The following example shows how to set a default domain name of FirstDomain for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes hostname(config-group-policy)# default-domain value FirstDomain
```

Defining a List of Domains for Split Tunneling

Enter a list of domains to be resolved through the split tunnel. Enter the **split-dns** command in group-policy configuration mode. To delete a list, enter the **no** form of this command.

When there are no split tunneling domain lists, users inherit any that exist in the default group policy. To prevent users from inheriting such split tunneling domain lists, enter the **split-dns** command with the **none** keyword.

To delete all split tunneling domain lists, enter the **no split-dns** command without arguments. This deletes all configured split tunneling domain lists, including a null list created by issuing the **split-dns** command with the **none** keyword.

The parameter **value** *domain-name* provides a domain name that the security appliance resolves through the split tunnel. The **none** keyword indicates that there is no split DNS list. It also sets a split DNS list with a null value, thereby disallowing a split DNS list, and prevents inheriting a split DNS list from a default or specified group policy. The syntax of the command is as follows:

```
hostname(config-group-policy)# split-dns {value domain-name1 [domain-name2... domain-nameN] | none} hostname(config-group-policy)# no split-dns [domain-name domain-name2 domain-nameN]
```

Enter a single space to separate each entry in the list of domains. There is no limit on the number of entries, but the entire string can be no longer than 255 characters. You can use only alphanumeric characters, hyphens (-), and periods (.). If the default domain name is to be resolved through the tunnel, you must explicitly include that name in this list.

The following example shows how to configure the domains Domain1, Domain2, Domain3, and Domain4 to be resolved through split tunneling for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-dns value Domain1 Domain2 Domain3 Domain4
```

Configuring DHCP Intercept

A Microsoft XP anomaly results in the corruption of domain names if split tunnel options exceed 255 bytes. To avoid this problem, the security appliance limits the number of routes it sends to 27 to 40 routes, with the number of routes dependent on the classes of the routes.

DHCP Intercept lets Microsoft Windows XP clients use split-tunneling with the security appliance. The security appliance replies directly to the Microsoft Windows XP client DHCP Inform message, providing that client with the subnet mask, domain name, and classless static routes for the tunnel IP address. For Windows clients prior to Windows XP, DHCP Intercept provides the domain name and subnet mask. This is useful in environments in which using a DHCP server is not advantageous.

The **intercept-dhcp** command enables or disables DHCP intercept. The syntax of this command is as follows:

[no] intercept-dhcp

```
hostname(config-group-policy)# intercept-dhcp netmask {enable | disable}
hostname(config-group-policy)#
```

The *netmask* variable provides the subnet mask for the tunnel IP address. The **no** version of the command removes the DHCP intercept from the configuration.

The following example shows how to set DHCP Intercepts for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes hostname(config-group-policy)# intercept-dhcp enable
```

Configuring Backup Server Attributes

Configure backup servers if you plan on using them. IPsec backup servers let a VPN client connect to the central site when the primary secure gateway is unavailable. When you configure backup servers, the security appliance pushes the server list to the client as the IPsec tunnel is established. Backup servers do not exist until you configure them, either on the client or on the primary secure gateway.

Configure backup servers either on the client or on the primary secure gateway. If you configure backup servers on the security appliance, it pushes the backup server policy to the clients in the group, replacing the backup server list on the client if one is configured.



If you are using hostnames, it is wise to have backup DNS and WINS servers on a separate network from that of the primary DNS and WINS servers. Otherwise, if clients behind a hardware client obtain DNS and WINS information from the hardware client via DHCP, and the connection to the primary server is

lost, and the backup servers have different DNS and WINS information, clients cannot be updated until the DHCP lease expires. In addition, if you use hostnames and the DNS server is unavailable, significant delays can occur.

To configure backup servers, enter the **backup-servers** command in group-policy configuration mode:

```
hostname(config-group-policy)# backup-servers {server1 server2... server10 |
clear-client-config | keep-client-config}
```

To remove a backup server, enter the **no** form of this command with the backup server specified. To remove the backup-servers attribute from the running configuration and enable inheritance of a value for backup-servers from another group policy, enter the **no** form of this command without arguments.

```
hostname(config-group-policy)# no backup-servers [server1 server2... server10 |
clear-client-config | keep-client-config]
```

The **clear-client-config** keyword specifies that the client uses no backup servers. The security appliance pushes a null server list.

The **keep-client-config** keyword specifies that the security appliance sends no backup server information to the client. The client uses its own backup server list, if configured. This is the default.

The server1 server 2.... server10 parameter list is a space-delimited, priority-ordered list of servers for the VPN client to use when the primary security appliance is unavailable. This list identifies servers by IP address or hostname. The list can be 500 characters long, and it can contain up to 10 entries.

The following example shows how to configure backup servers with IP addresses 10.10.10.1 and 192.168.10.14, for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# backup-servers 10.10.10.1 192.168.10.14
```

Configuring Address Pools

Configure a list of address pools for allocating addresses to remote clients by entering the **address-pools** command in group-policy attributes configuration mode:

```
hostname(config-group-policy)# address-pools value address_pool1 [...address_pool6] hostname(config-group-policy)#
```

The address-pools settings in this command override the local pool settings in the group. You can specify a list of up to six local address pools to use for local address allocation.

The order in which you specify the pools is significant. The security appliance allocates addresses from these pools in the order in which the pools appear in this command.

To remove the attribute from the group policy and enable inheritance from other sources of group policy, use the **no** form of this command:

```
hostname(config-group-policy) # no address-pools value address_pool1 [...address_pool6] hostname(config-group-policy) #
```

The command **address-pools none** disables this attribute from being inherited from other sources of policy, such as the DefaultGrpPolicy:

```
hostname(config-group-policy)# address-pools none
hostname(config-group-policy)#
```

The command **no address pools none** removes the **address-pools none** command from the configuration, restoring the default value, which is to allow inheritance.

```
hostname(config-group-policy)# no address-pools none
hostname(config-group-policy)#
```

The syntax elements of this command are as follows:

- address_pool—Specifies the name of the address pool configured with the **ip local pool** command. You can specify up to 6 local address pools.
- none—Specifies that no address pools are configured and disables inheritance from other sources
 of group policy.
- value—Specifies a list of up to 6 address pools from which to assign addresses.

The following example entered in config-general configuration mode, configures pool 1 and pool 20 as lists of address pools to use for allocating addresses to remote clients for GroupPolicy1:

```
hostname(config) # ip local pool 192.168.10.1-192.168.10.100 mask 255.255.0.0 hostname(config) # ip local pool pool20 192.168.20.1-192.168.20.200 mask 255.255.0.0 hostname(config) # group-policy GroupPolicy1 attributes hostname(config-group-policy) # address-pools value pool1 pool20 hostname(config-group-policy) #
```

Configuring Firewall Policies

A *firewall* isolates and protects a computer from the Internet by inspecting each inbound and outbound individual packet of data to determine whether to allow or drop it. Firewalls provide extra security if remote users in a group have split tunneling configured. In this case, the firewall protects the user's PC, and thereby the corporate network, from intrusions by way of the Internet or the user's local LAN. Remote users connecting to the security appliance with the VPN client can choose the appropriate firewall option.

Set personal firewall policies that the security appliance pushes to the VPN client during IKE tunnel negotiation by using the **client-firewall** command in group-policy configuration mode. To delete a firewall policy, enter the **no** form of this command.

To delete all firewall policies, enter the **no client-firewall** command without arguments. This command deletes all configured firewall policies, including a null policy if you created one by entering the **client-firewall** command with the **none** keyword.

When there are no firewall policies, users inherit any that exist in the default or other group policy. To prevent users from inheriting such firewall policies, enter the **client-firewall** command with the **none** keyword.

The Add or Edit Group Policy window, Client Firewall tab, lets you configure firewall settings for VPN clients for the group policy being added or modified.



Only VPN clients running Microsoft Windows can use these firewall features. They are currently not available to hardware clients or other (non-Windows) software clients.

In the first scenario, a remote user has a personal firewall installed on the PC. The VPN client enforces firewall policy defined on the local firewall, and it monitors that firewall to make sure it is running. If the firewall stops running, the VPN client drops the connection to the security appliance. (This firewall enforcement mechanism is called *Are You There (AYT)*, because the VPN client monitors the firewall by sending it periodic "are you there?" messages; if no reply comes, the VPN client knows the firewall is

down and terminates its connection to the security appliance.) The network administrator might configure these PC firewalls originally, but with this approach, each user can customize his or her own configuration.

In the second scenario, you might prefer to enforce a centralized firewall policy for personal firewalls on VPN client PCs. A common example would be to block Internet traffic to remote PCs in a group using split tunneling. This approach protects the PCs, and therefore the central site, from intrusions from the Internet while tunnels are established. This firewall scenario is called *push policy* or *Central Protection Policy (CPP)*. On the security appliance, you create a set of traffic management rules to enforce on the VPN client, associate those rules with a filter, and designate that filter as the firewall policy. The security appliance pushes this policy down to the VPN client. The VPN client then in turn passes the policy to the local firewall, which enforces it.

Enter the following commands to set the appropriate client firewall parameters. You can configure only one instance of this command. Table 3-1, following this set of commands, explains the syntax elements of these commands:

Cisco Integrated Firewall

 $\label{local_continuous} \mbox{hostname} \mbox{ (config-group-policy) \# client-firewall \{opt \mid req\} cisco-integrated acl-in ACL acl-out ACL }$

Cisco Security Agent

hostname(config-group-policy)# client-firewall {opt | req} cisco-security-agent

No Firewall

hostname(config-group-policy)# client-firewall none

Custom Firewall

 $\label{local_config} $$ hostname(config-group-policy) \# \ client-firewall \{opt \mid req\} \ custom \ vendor-id \ num \ product-id \ num \ policy \{AYT \mid CPP \ acl-in \ ACL \ acl-out \ ACL\} \ [description \ string] $$$

Zone Labs Firewalls



 $\verb|hostname| (config-group-policy) # \verb| client-firewall {opt | req}| | zonelabs-integrity| \\$

When the firewall type is **zonelabs-integrity**, do not include arguments. The Zone Labs Integrity Server determines the policies.

hostname(config-group-policy)# client-firewall {opt | req} zonelabs-zonealarm policy {AYT | CPP acl-in ACL acl-out ACL}

 $\label{local_problem} $$ \operatorname{hostname}(\operatorname{config-group-policy}) \# \operatorname{client-firewall} \{ opt \mid \operatorname{req} \} \ \operatorname{zonelabs-zonealarmorpro} \operatorname{policy} \{ \operatorname{AYT} \mid \operatorname{CPP} \operatorname{acl-in} \operatorname{ACL} \operatorname{acl-out} \operatorname{ACL} \}$

Sygate Personal Firewalls

```
hostname(config-group-policy)# client-firewall {opt | req} sygate-personal
hostname(config-group-policy)# client-firewall {opt | req} sygate-personal-pro
hostname(config-group-policy)# client-firewall {opt | req} sygate-security-agent
```

Network Ice, Black Ice Firewall:

hostname(config-group-policy)# client-firewall {opt | req} networkice-blackice

Table 3-1 client-firewall Command Keywords and Variables

Parameter	Description		
acl-in ACL	Provides the policy the client uses for inbound traffic.		
acl-out ACL	Provides the policy the client uses for outbound traffic.		
AYT	Specifies that the client PC firewall application controls the firewall policy. The security appliance checks to make sure that the firewall is running. It asks, "Are You There?" If there is no response, the security appliance tears down the tunnel.		
cisco-integrated	Specifies Cisco Integrated firewall type.		
cisco-security-agent	Specifies Cisco Intrusion Prevention Security Agent firewall type.		
CPP	Specifies Policy Pushed as source of the VPN client firewall policy.		
custom	Specifies Custom firewall type.		
description string	Describes the firewall.		
networkice-blackice	Specifies Network ICE Black ICE firewall type.		
none	Indicates that there is no client firewall policy. Sets a firewall policy with a null value, thereby disallowing a firewall policy. Prevents inheriting a firewall policy from a default or specified group policy.		
opt	Indicates an optional firewall type.		
product-id	Identifies the firewall product.		
req	Indicates a required firewall type.		
sygate-personal	Specifies Sygate Personal firewall type.		
sygate-personal-pro	Specifies Sygate Personal Pro firewall type.		
sygate-security-agent	Specifies Sygate Security Agent firewall type.		
vendor-id	Identifies the firewall vendor.		
zonelabs-integrity	Specifies Zone Labs Integrity Server firewall type.		
zonelabs-zonealarm	Specifies Zone Labs Zone Alarm firewall type.		
zonelabs-zonealarmorpro policy	Specifies Zone Labs Zone Alarm or Pro firewall type.		
zonelabs-zonealarmpro policy	Specifies Zone Labs Zone Alarm Pro firewall type.		

The following example shows how to set a client firewall policy that requires Cisco Intrusion Prevention Security Agent for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-firewall req cisco-security-agent
hostname(config-group-policy)#
```

Configuring Client Access Rules

Configure rules that limit the remote access client types and versions that can connect via IPsec through the security appliance by using the **client-access-rule** command in group-policy configuration mode. Construct rules according to these guidelines:

- If you do not define any rules, the security appliance permits all connection types.
- When a client matches none of the rules, the security appliance denies the connection. If you define
 a deny rule, you must also define at least one permit rule; otherwise, the security appliance denies
 all connections.
- For both software and hardware clients, type and version must exactly match their appearance in the **show vpn-sessiondb remote** display.
- The * character is a wildcard, which you can enter multiple times in each rule. For example, client-access rule 3 deny type * version 3.* creates a priority 3 client access rule that denies all client types running release versions 3.x software.
- You can construct a maximum of 25 rules per group policy.
- There is a limit of 255 characters for an entire set of rules.
- You can enter n/a for clients that do not send client type and/or version.

To delete a rule, enter the **no** form of this command. This command is equivalent to the following command:

```
\verb|hostname| (config-group-policy) # client-access-rule 1 deny type "Cisco VPN Client" version 4.0
```

To delete all rules, enter the **no client-access-rule command** without arguments. This deletes all configured rules, including a null rule if you created one by issuing the **client-access-rule** command with the **none** keyword.

By default, there are no access rules. When there are no client access rules, users inherit any rules that exist in the default group policy.

To prevent users from inheriting client access rules, enter the **client-access-rule** command with the **none** keyword. The result of this command is that all client types and versions can connect.

```
\label{loss_prop_policy} $$ hostname(config-group-policy) $$ $$ $ $ $ client-access rule $priority $$ $ \{permit \mid deny\} $ $      type $$      version $$ \{version \mid none\}$ $$
```

 $\label{loss_prop_policy} \mbox{hostname} \mbox{ (config-group-policy) \# no client-access rule } \mbox{ [$priority$ \{$permit \mid deny$\} type type version $version$]}$

Table 3-2 explains the meaning of the keywords and parameters in these commands.

Table 3-2	client-access rule Command Keywords and Variables

Parameter	Description		
deny	Denies connections for devices of a particular type and/or version.		
none	Allows no client access rules. Sets client-access-rule to a null value, thereby allowing no restriction. Prevents inheriting a value from a default or specified group policy.		
permit	Permits connections for devices of a particular type and/or version.		
priority	Determines the priority of the rule. The rule with the lowest integer has the highest priority. Therefore, the rule with the lowest integer that matches a client type and/or version is the rule that applies. If a lower priority rule contradicts, the security appliance ignores it.		
type type	Identifies device types via free-form strings, for example VPN 3002. A string must match exactly its appearance in the show vpn-sessiondb remote display, except that you can enter the * character as a wildcard.		
version version	Identifies the device version via free-form strings, for example 7.0. A string must match exactly its appearance in the show vpn-sessiondb remote display, except that you can enter the * character as a wildcard.		

The following example shows how to create client access rules for the group policy named FirstGroup. These rules permit Cisco VPN clients running software version 4.x, while denying all Windows NT clients:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-access-rule 1 deny type WinNT version *
hostname(config-group-policy)# client-access-rule 2 permit "Cisco VPN Client" version 4.*
```



The "type" field is a free-form string that allows any value, but that value must match the fixed value that the client sends to the security appliance at connect time.

Example: Configuring a Security Appliance for the VPN Client Using CLI

The following example shows one way of configuring a security appliance for a VPN Client connection. the commands specifically relevant to the VPN Client are highlighted in bold type:

```
group-policy Engineering attributes

vpn-tunnel-protocol IPsec

configure terminal

tunnel-group TestTunnelGroup1 general-attributes

accounting-server-group ACS-1

default-group-policy Engineering

strip-group

strip-realm

no dhcp-server 209.165.200.200

dhcp-server 209.165.200.201

override-account-disable

password-management password-expire-in-days 0

authentication-server-group (inside) ACS-1 LOCAL
```

```
authentication-server-group ACS-1 LOCAL
  authorization-server-group (inside) ACS-1
  authorization-server-group LOCAL
  address-pool (test) Engineering
tunnel-group TestTunnelGroup1 ipsec-attributes
  chain
  pre-shared-key *******
  isakmp keepalive disable
  trust-point ASDM TrustPoint11
  client-update type Windows url http://www.cisco.com rev-nums 4.6,4.7,4.8,4.9,5.0
  client-update type vpn3002 url tftp://www.cisco.com rev-nums 4.6
 client-update type asa5505 component image url https://www.cisco.com rev-nums 7.2
  isakmp ikev1-user-authentication (inside) hybrid
tunnel-group TestTunnelGroup1 ppp-attributes
  authentication ms-chap-v2
vpn-addr-assign local reuse-delay 5
group-delimiter #
```



CHAPTER 4

Configuring the VPN Client on a VPN 3000 Series Concentrator

This chapter describes how to configure the VPN Client parameters on a Cisco VPN 3000 Series Concentrator. As with the other chapters, this one focuses on those parameters that you must configure specifically for the VPN Client. For complete information about configuration using the CLI, see *VPN 3000 Series Concentrator Reference Volume I: Configuration*.

The general considerations are the same for both the CLI and ASDM, in that you must configure the following parameters for the VPN Client:

- Configure the IPsec connection profile.
- Configure the advanced IPsec features.
- Configure Client Update.

This chapter includes the following major topics:

- Configuring the VPN Client on a VPN 3000 Series Concentrator, page 4-1
- Configuring VPN Client Users for Digital Certificate Authorization, page 4-4
- Configuring VPN Client Firewall Policy for Windows, page 4-10
- Notifying Remote Users of a Client Update—All VPN Client Platforms, page 4-19
- Setting up Local LAN Access for the VPN Client, page 4-20
- Configuring the VPN Concentrator for Client Backup Servers, page 4-22
- Configuring NAT Traversal for the VPN Client, page 4-22
- Configuring Automatic Browser Configuration—Windows Only, page 4-23
- Configuring Entrust Entelligence for the VPN Client—Windows Only, page 4-24
- Setting up the VPN Client for Authentication using Smart Cards—Windows Only, page 4-26
- Configuring Mutual Authentication, page 4-27

Configuring the VPN Client on a VPN 3000 Series Concentrator

We recommend that you carefully read the chapter on "User Management," *VPN 3000 Series Concentrator Reference Volume I: Configuration.* The "User Management" chapter contains complete information on setting up remote users to connect through the IPsec tunnel, and also explains how to use features such as setting up a client banner, firewalls, split tunneling, and so on.

This section covers the following tasks:

- Completing Quick Configuration, page 4-2
- Creating an IPsec Group, page 4-3
- Certificate Distinguished Name Matching, page 4-6
- Certificate Key Usage, page 4-7
- Certificate Fall Through, page 4-8
- Connecting with Digital Certificates, page 4-9
- Overview of Using Personal Client Firewalls, page 4-10
- VPN Client for Linux Firewall Configuration, page 4-12
- Firewall Configuration Scenarios, page 4-13
- Defining a Filter and Rules to Use with Firewalls for CPP, page 4-15Obtaining Firewall Troubleshooting Information, page 4-17
- Global Configuration, page 4-22
- Tear Down Tunnel When Smart Card Is Removed, page 4-26
- Notify User When a Smart Card Is Locked for Too Many Bad PINs, page 4-26
- Smart Card Password Reprompt for New Connections, page 4-27
- Configuring Mutual Group Authentication on the VPN Client System, page 4-27
- Configuring Mutual Authentication on the VPN Concentrator, page 4-28

Completing Quick Configuration

For steps in quick configuration, refer to *Cisco VPN 3000 Series Concentrator Getting Started* or Quick Configuration online help.

Be sure to perform the following tasks.

- Configure and enable both Ethernet interfaces 1 and 2 (Private and Public) with appropriate IP addresses and filters.
- Configure a DNS server and default gateway.
- Enable IPsec as one of the tunneling protocols (the default).
- Enter a group name and password for an IPsec group.
- Configure at least one method for assigning user IP addresses.



Note

If split or excluded tunnels are to be configured, ensure that the proper mask is assigned to the address pool or assigned IP address. By default, a classful mask is applied to the virtual adapter capable clients, and this default mask might cause the client to tunnel unintended traffic.

- Configure authentication servers for group and user authentication. These instructions assume the internal server for both, but you can set up any of the external servers instead.
- · Save the configuration.

Creating an IPsec Group

During the Quick Configuration, you can automatically create an IPsec group. If you want to add an IPsec group or modify one, follow the procedure in this section.

Refer to "User Management" in VPN 3000 Series Concentrator Reference Volume I: Configuration for details about configuring groups.

You might want to set base-group attributes before you create an IPsec group:

- For ASDM, see the ASDM Configuration > Remote Access VPN > Network (Client) Access > IPsec Connection Profiles window
- For the VPN 3000 Concentrator, see the Configuration | User Management | Base Group screen.

We suggest you carefully review the IPsec Connection Parameters (ASDM) or the General Parameters and IPsec Parameters (VPN 3000 Concentrator) on those windows.

If you use external user authentication, default or base-group attributes are especially important since they govern all attributes that the external server does not provide.

The VPN Client uses the IPsec protocol for creating and using secure tunnels. IPsec has two authentication phases: first for the group, then for the user. These instructions assume that you are using the VPN 3000 Concentrator internal authentication server for both group and user authentication.

Use the Configuration | User Management | Groups | Add screen to create an IPsec group:

- Step 1 Under the Identity tab, enter a Group Name and Password. VPN Client users need these to configure a connection entry and connect via the VPN Client; see "Gathering Information You Need" in Chapter 2 of the VPN Client User Guide for your platform.
- Step 2 Next, select a method of authentication. The Type parameter determines the group authentication method, Internal or External. Internal groups are configured on the VPN Concentrator. If you select External, you must configure an external RADIUS server to authenticate and provide appropriate group attributes.
- Step 3 Under the General tab | Tunneling Protocols, be sure IPsec is checked.
- Step 4 Under the IPsec tab | IPsec SA, select ESP-3DES-MD5 to require Triple-DES authentication.

 Alternatively, you could choose ESP-DES-MD5, which uses DES authentication and provides a minimum level of security. Or, to use AES, select one of the AES protocols, such as ESP-AES128-SHA. AES is the most secure.



Note

To create or customize the Security Association (SA), see the Configuration | Policy Management | Traffic Management | Security Associations screens.

- Step 5 Under IPsec > Authentication, choose the method you use for the members of the group; for example, Internal or RADIUS. If you choose an authentication method other than None or Internal, be sure to configure the external authentication server appropriately and supply users with the appropriate information for installing the VPN Client.
- Step 6 To require users to enter a password each time they log in, we suggest that you *not* check Allow Password Storage on the Client, which is on the Client Config tab. Not checking this parameter provides greater security.
- Step 7 To add the group, click **Add**, and then save the configuration.

Creating VPN Client User Profiles

For details on configuring VPN Client users within a group, see "User Management," in the VPN 3000 Series Concentrator Reference Volume 1: Configuration.

Use the Configuration | User Management | Users | Add or Modify screen to configure a VPN Client user:

Step 1 Enter a User Name, Password, and Verify Password. VPN Client users need a user name and password to authenticate when they connect to the VPN Concentrator; see "Gathering Information You Need" in Chapter 2 of the VPN Client User Guide for your platform.



Beginning with Release 4.6.04.x, the VPN Client can accept a pre-shared password of up to 128 characters. The VPN 3000 Concentrator, however, imposes a limit of 32 characters.

- Step 2 Under Group, select the group name you configured under the section "Creating an IPsec Group."
- Step 3 Carefully review and configure other attributes under General and IPsec. Note that if you are adding a user, the Inherit? checkboxes refer to base-group attributes; if you are modifying a user, the checkboxes refer to the user's assigned-group attributes.
- Step 4 Click Add or Apply, and save the configuration.

Configuring VPN Client Users for Digital Certificate Authorization

Use the following procedure to configure the VPN 3000 Concentrator for IPsec client connections using digital certificates.

- Activate an IKE SA.
- Configure a security association (SA) to use the VPN 3000 Concentrator's identity certificate.
- Create a new group for clients connecting with certificates.
- Add VPN Client users to the new group.
- For details refer to the VPN 3000 Series Concentrator Reference Volume I: Configuration:
 - On configuring IKE proposals, see "Tunneling Protocols."
 - On configuring SAs, see "Policy Management."
 - On configuring groups and users, see "User Management."

Follow these steps:

- Step 1 Use the Configuration | System | Tunneling Protocols | IPsec | IKE Proposals screen to activate an IKE proposal for certificates:
 - a. Activate one of the IKE protocols such as Cisco VPN Client-3DES-MD5-RSA-DH5, Cisco VPN Client-3DES-SHA-DSA-DH5, or Cisco VPN Client-AES128-SHA.



Note

To use AES, move the AES proposal(s) to the top of the list. You must be running Release 3.6 or higher of the VPN Client software to use AES.

- b. If you do not want to modify one of the standard proposals, copy an active proposal and give it a new name; for example, copy the Cisco VPN Client-3DES-MD5-RSA-DH5 and name it "IKE-Proposal for digital certificate use."
- c. Click Security Associations, which takes you to the next step.
- Use the Configuration | Policy Management | Traffic Management | Security Associations screen to Step 2 create a new SA. You can use the Security Associations link on the IKE Proposals screen.
 - a. Add a new SA. For example, name it "Security association for digital certificate use."
 - b. Change the Digital Certificates parameter to identify the VPN 3000 Concentrator's digital certificate. This is the only field that you need to change.
- Step 3 Use the Configuration | User Management | Groups | Add or Modify screen to configure a group for using digital certificates:
 - a. To use the Organizational Unit to configure the group, under the Identity tab, enter a group name that is the same as the OU field of the certificate(s) for this group. For example, if the OU in the VPN Client certificate is Finance, you would enter Finance as the group name. The OU is a field of the ASN.1 Distinguished Name (DN). Enter password and verify it.
 - Alternatively, you can configure a policy for certificate group matching. To use this approach, go to Configuration | Policy Management | Certificate Group Matching | Policy. For instructions on creating rules, see VPN 3000 Series Concentrator Reference I: Configuration for this section or refer to online help.
 - b. Under the IPsec tab > IPsec SA, select the IPsec SA you created in step 2; for example, "Security association for digital certificate use."
 - c. Under IPsec tab > Authentication, select the method you use for user authentication; for example, Internal. If you select an external authentication method, such as RADIUS, be sure to configure the external authentication server appropriately and supply users with the appropriate entries for the "Gathering the Information You Need" section in Chapter 2 of the VPN Client User Guide for your platform.
 - **d.** Click **Add** or **Apply**, and save the configuration.
- Step 4 Use the Configuration | User Management | Users | Add or Modify | Identity screen to configure VPN Client users for digital certificates:
 - a. As the group name, enter the group you have set up in step 3 as the group parameter; continuing the example, you would enter Finance.
 - b. Click **Add** or **Apply**, and save the configuration.
 - New Certificate features to dynamically map a Certificate to a profile without manual selection by the user:
 - Certificate Distinguished name Matching (Windows and Linux)
 - Certificate Key Usage (Windows, Linux, and Mac)
 - Certificate Fall-Through (Windows and Linux)

The following sections describe these features.

Certificate Distinguished Name Matching

For Windows and Linux platforms, the Profile Keyword: CertMatchDN parameter specifies the wildcard string to match and selects a particular certificate by its Distinguished Name, in the given certificate store, during a connection attempt. If the wildcard string matches multiple certificates, the first certificate that satisfies the wildcard string is chosen. The value of this parameter is a pseudo-regular expression, the format of which is exactly identical to that of the VerifyCertDN profile keyword.

Valid keywords for the wildcard string are:

- "CN" SubjectCommonName
- "SN" SubjectSurName
- "GN" SubjectGivenName
- "N" SubjectUnstructName
- "I" SubjectInitials
- "GENQ" SubjectGenQualifier
- "DNQ" SubjectDnQualifier
- "C" SubjectCountry
- "L" SubjectCity
- "SP" SubjectState
- "ST" SubjectState
- "O" SubjectCompany
- "OU" SubjectDept
- · "T" SubjectTitle
- "EA" SubjectEmailAddr
- "ISSUER-CN" IssuerCommonName
- "ISSUER-SN" IssuerSurName
- "ISSUER-GN" IssuerGivenName
- "ISSUER-N" IssuerUnstructName
- "ISSUER-I" IssuerInitials
- · "ISSUER-GENQ" IssuerGenQualifier
- · "ISSUER-DNQ" IssuerDnQualifier
- · "ISSUER-C" IssuerCountry
- · "ISSUER-L" IssuerCity
- "ISSUER-SP" IssuerState
- "ISSUER-ST" IssuerState
- "ISSUER-O" IssuerCompany
- "ISSUER-OU" IssuerDept
- "ISSUER-T" IssuerTitle
- "ISSUER-EA" IssuerEmailAddr

Example:

```
CertMatchDN=CN="ID Cert",OU*"Cisco",ISSUER-CN!="Entrust",ISSUER-OU!*"wonderland" CN="ID Cert"--Specifies an exact match on the CN.

OU*"Cisco"--Specifies any OU that contains the string "Cisco".

ISSUER-CN!"Entrust"--Specifies that the Issuer CN must not equal "Entrust".

ISSUER-OU!*"wonderland"--Specifies that the Issuer OU must not contain "wonderland".
```

Certificate Key Usage

For Windows, Linux, and Mac platforms, the global parameter vpnent.ini [Main] keyword: CertificateKeyUsage restricts the usage of Certificates from all stores to only those with the Certificate Key Usage parameters: Digital Signature or Non-Repudiation.

If the "CertificateKeyUsage=1" when the client is launched, only Certificates with the proper key usage are displayed under the Certificates tab. In addition, profiles configured to use Certificates that do not have the proper key usage receive an error that the Certificate cannot be found.

The default for this keyword is "CertificateKeyUsage=0", which allows all available Certificates to be selected and used.

This keyword overrides all other Certificate matching criteria, such as CertMatchDN.

Certificate Key Usage Matching

For Windows and Linux platforms, the Certificate Key Usage Matching feature allows the profile selection of Certificates based on the Key Usage as well as the DN and Extended Key Usage fields. The Profile Keyword: CertMatchKU overrides the vpnent.ini keyword "CertificateKeyUsage".

For example:

```
CertMatchKU=0,3,4,5

DIGITAL_SIGNATURE 8

NON_REPUDIATION 7

KEY_ENCIPHERMENT 6

DATA_ENCIPHERMENT 5

KEY_AGREEMENT 4

KEY_CERT_SIGN 3

CRL_SIGN 2

ENCIPHER_ONLY 1

DECIPHER_ONLY 0
```

If the Certificate matches any of the usages in the CertMatchKU field, it passes on to the next criterion. Otherwise, the Certificate is not selected.

If two Certificates, identical except for Key Usage, are available to the following profile, only the one with Non-Repudiation is chosen.

```
[Main]
Host=1.2.3.4
AuthType=3
CertStore=2
CertName=myMultipleCerts
CertMatchKU=7
!CertSubjectName=
!CertSerialHash=
```

Certificate Extended Key Usage Matching

The profile keyword parameter CertMatchEKU specifies the list of extended Key Usage fields that the VPN Client should honor. When this profile keyword is specified, during a connection attempt the VPN Client looks only at those certificates (irrespective of certificate store) whose Extended Key Usage fields match those that are specified by the profile keyword. That is, when this profile keyword is specified, for any given certificate, at least one of the Extended Key Usage fields specified in the profile keyword must be present in the certificate's Extended key Usage field.

This keyword applies to connection attempts only and not to any other certificate-related operation (such as listing certificates, viewing certificates, and so on). This keyword applies to all forms of certificate selection (such as CertSerialHash, CertMatchDN, CertSubjectName, or CertName). The value of this keyword is a comma-separated list of Extended Key Usage OID strings. Custom Extended Key Usage strings must be of the form 1.3.6.1.5.5.7.3.n, where n can be any number.

For example:

```
CertMatchEKU=1.3.6.1.5.5.7.3.2,1.3.6.1.5.5.7.3.1 where:

1.3.6.1.5.5.7.3.2 = Client authentication

1.3.6.1.5.5.7.3.1 = Server Authentication
```

Certificate Fall Through

For a given connection attempt, you can select a certificate using one or more of the keywords given below (in order of precedence).

- 1. CertSerialHash
- 2. CertMatchDN
- 3. CertSubjectName
- 4. CertName

If the VPN Client cannot find a certificate in the given cent store using all of the Certificate keywords noted above, the connection attempt fails.

This behavior is implicit and does not have any profile keyword associated with it.

The following is a sample profile:

```
[Main]
Host=10.10.10.10
AuthType=3
CertStore=2
!UserName=
!UserPassword=
CertMatchDN=issuer-ou*"vpn group",ea*"Cisco.com"
!CertSerialHash=
```

This profile matches only certificates that have a Key Usage of "Non-Repudiation" and have either Client or Server Authentication in the Extended Key Usage. The Issuer-ou field must contain "vpn group", and the email address for the user Certificate must contain "cisco.com" (case insensitive).

In the Windows environment (the VPN Clients for Linux and Mac do not support smart cards), the preceding scenario allows a common workstation to connect users based on their smart card certificates. A user could walk up, insert the smart card, and press connect. This generic profile would find the proper

certificate on the card (without restarting the client or modifying the profile) and prompt the user for his or her Certificate password, username, and password. The secure gateway could also be configured to connect without a username and rely entirely upon the Certificates for authentication.



The use of the "!" character in the profile prevents the previous user's information from being retained between connections.

Certificate Matching matches the first available Certificate that matches the rules set up for Certificate Matching, regardless of validity, causing the connection to fail. To prevent expired certificates from being selected when valid ones are available, the Windows VPN Client now ignores invalid or expired Certificates from the Certificate Store. (CSCsd38373, CSCsd38360).

Important Note about Using CertSerialHash

When using DN or other match criteria to find a certificate such as the example below:

CertMatchDN=CN*"User"
!CertSerialHash=

the Client cannot update the serial hash value because the exclamation point (!) in front of the key word makes CertSerialHash a read-only field. Without the correct serial hash, the Client cannot create a watch timer to verify the existence of the Smartcard.

Without "!CertSerialHash=", the Client updates the cert hash with the certificate in the store and adds following line into the profile:

CertSerialHash=...03CF...

If a serial hash value already exists in the profile, such as "CertSerialHash=0102...xyz", and if you use a different Smartcard with a different certificate that matches the DN, the Smartcard watch also starts, but IPsec updates the serial hash value of the CertSerialHash parameter to that of the certificate being used.



It's essential *not* to use '!' in front of "CertSerialHash=" in this context, because you must allow the VPN Client to update the serial hash value to the intended certificate.

Connecting with Digital Certificates

Before you create a VPN Client connection entry using a digital certificate, you must have already enrolled in a Public Key Infrastructure (PKI), have received approval from the Certificate Authority (CA), and have one or more certificates installed on the VPN Client system. If this is not the case, then you need to obtain a digital certificate. You can obtain one by enrolling with a PKI directly using the Certificate Manager feature, or you can obtain an Entrust profile through Entrust Entelligence. Currently, we have tested the following PKIs:

- UniCERT from Baltimore Technologies (www.baltimoretechnologies.com)
- Entrust PKITM 5.0 from Entrust Technologies (www.entrust.com)
- Versign (www.verisign.com)
- RSA KEON 5.7 and 6.0
- Microsoft Certificate Services 2.0

· Cisco Certificate Store

The Web sites listed in parentheses in this list contain information about the digital certificates that each PKI provides.

Configuring VPN Client Firewall Policy for Windows

To provide a higher level of security, the VPN Client can either enforce the operation of a supported firewall or receive a pushed down stateful firewall policy for Internet bound traffic. This section includes the following topics:

- · How firewalls work with the VPN Client.
- List of the personal firewall products that the VPN Client can enforce for Internet traffic.
- How to configure a stateful firewall policy on a VPN Concentrator for the VPN Client to enforce.

Overview of Using Personal Client Firewalls

This section summarizes how a network administrator can control personal firewall features from a VPN 3000 Concentrator operating as the secure gateway communicating policy information to the VPN Client running on a Windows platform.

Optional versus Required Configuration Option

The VPN Concentrator can require that a VPN Client use a designated firewall configuration or make this configuration optional. Making a designated firewall configuration optional gives a VPN Client user a chance to install the desired firewall on the client PC. When the VPN Client tries to connect, it notifies the VPN Concentrator about any firewalls installed on the client PC. The VPN Concentrator sends back information about what firewall the VPN Client must use. If the firewall configuration is optional, the VPN Concentrator can notify the VPN Client that there is a mismatch but still allow the VPN Client to establish a tunnel. The optional feature thus lets the network administrator of the VPN Client maintain the tunneled connection while obtaining and installing the required firewall.

Stateful Firewall (Always On)

The VPN Client configuration option Stateful Firewall (Always On) is enabled on the VPN Client. This configuration option is not negotiated. The policy is not controlled from the VPN Concentrator. The VPN Client user enables this option on the VPN Client under the Options menu or while the VPN Client is active by right-clicking on the VPN Client icon and selecting the option.

When enabled, this feature allows no inbound sessions from all networks, whether or not a VPN connection is in effect. Also, the firewall is active for both tunneled and nontunneled traffic. Users who enable this feature cannot have a server running on their PC and their system can no longer respond to PING requests. There are two exceptions to allowing no inbound traffic. The first is DHCP, which sends requests to the DHCP server out one port but receives responses from DHCP through a different port. For DHCP, the stateful firewall allows inbound traffic. The second is ESP (VPN data). The stateful firewall allows ESP traffic from the secure gateway, because ESP rules are packet filters and not session-based filters.

Stateful Firewall (Always On) is the most basic VPN Client firewall and provides the highest level of security. However, it is also the least flexible, since it blocks almost all incoming traffic and does not allow outbound traffic to be limited.



The Always On personal firewall allows inbound access from the internal (tunneled) network to ensure that your internal applications work properly, while still providing additional protection for non tunneled traffic.

Cisco Integrated Client

The VPN Client on the Windows platform includes a stateful firewall that incorporates Zone Labs technology. This firewall is used for both the Stateful Firewall (Always On) feature and the Centralized Protection Policy (see "Centralized Protection Policy (CPP)"). This firewall is transparent to the VPN Client user, and is called "Cisco Integrated Client Firewall" or CIC. While the "Always On" option lets the VPN Client user choose to have basic firewall protection in effect, CPP lets an administrator define rules to enforce for inbound/outbound Internet traffic during split tunneling operation. Since tunnel everything already forces all traffic back through the tunnel, CPP is not used for tunnel everything.

Centralized Protection Policy (CPP)

Centralized Protection Policy (CPP) also known as firewall *push policy*, lets a network administrator define a set of rules for allowing or dropping Internet traffic while the VPN Client is tunneled in to the VPN Concentrator. A network administrator defines this policy on the VPN Concentrator, and the policy is sent to the VPN Client during connection negotiation. The VPN Client passes the policy to the Cisco Integrated Client, which then enforces the policy. If the client user has already selected the "Always On" option, any more restrictive rules are enforced for Internet traffic while the tunnel is established.

Since CIC includes a stateful firewall module, most configurations block all inbound traffic and permit either all outbound traffic or traffic through specific TCP and UDP ports outbound. Cisco Integrated Client, Zone Alarm, and Zone Alarm Pro firewalls can assign firewall rules. CPP rules are in effect during split tunneling and help protect the VPN Client PC from Internet attacks by preventing servers from running and by blocking any inbound connections unless they are associated with outbound connections.

CPP provides more flexibility than the Stateful Firewall (Always On) feature, since with CPP, you can refine the ports and protocols that you want to permit.

Policy Configured on the Remote PC—Personal Firewall Enforcement

As an alternative to CPP, a network manager can define policy on the personal firewall that is installed on the same PC as the VPN Client. This approach accommodates situations where there is already a firewall set up and in use on the PC. The VPN Client then polls the personal firewall every 30 seconds to make sure it is running and if it is not, terminates the secure connection to the VPN Concentrator. In this case, the VPN Concentrator does not define the firewall policy. The only contact the VPN Client has with the firewall is polling it to ascertain that it is running, a capability known as Are You There (AYT).

Currently, the VPN Client supports the following personal firewalls:

- · BlackIce Defender
- · Cisco Security Agent
- Sygate Personal Firewall

- · Sygate Personal Firewall Pro
- Sygate Security Agent
- ZoneAlarm
- ZoneAlarmPro

Zone Labs Integrity Agent and Integrity Server (IA/IS)

The Zone Labs Integrity solution secures remote PCs on Windows platforms. This feature is a client/server solution that comprises four components:

- Integrity Server (IS)—located on a central organization's network, IS maintains policies for the firewall on the remote VPN Client PCs. A network manager defines the policy on the IS, the IS downloads the policy to the Integrity Agent (IA) on the remote PC through a secure tunnel activated through the VPN Concentrator. The IS monitors the PC to ensure enforcement of the policy. The IS also communicates with the VPN Concentrator to establish/terminate connections, exchange session and user information, and report status information.
- Integrity Agent (IA)—on the remote PC enforces the protection policies it receives from IS and communicates with IS to exchange policy and status information. The IA also communicates with the VPN Client on the remote PC to obtain server addresses and to exchange status information with the VPN Concentrator.
- VPN Concentrator—provides the means for configuring firewall functionality by group. It reports
 the IS's IP address and other VPN session-related information to the VPN Client, which passes it on
 to the IA. The VPN Concentrator also communicates with the IS to establish and terminate sessions,
 exchange session and user information, and request and acquire authentication status.
- VPN Client—on the remote PC gets the IS addresses and information from the VPN Concentrator
 and passes it to the IA. The VPN Client also gets and reports status information from the IA and
 terminates sessions.

Once the connection is up and IS has communicated the firewall policy to IA, then IS and IA keep in touch though a heartbeat mechanism.

VPN Client for Linux Firewall Configuration

Cisco Systems provides the following firewall configuration, designed specifically for the VPN Client for Linux, Release 4.7.00.640, Virtual adapter. This code blocks all traffic on eth0, except for tunneled traffic.

```
# Firewall configuration written by Cisco Systems
# Designed for the Linux VPN Client 4.7.00.0640 Virtual Adapter
# Blocks ALL traffic on eth0 except for tunneled traffic

*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]

# Allow all traffic in both directions through the VA adapter
-A INPUT -i cipsec0 -j ACCEPT
-A OUTPUT -o cipsec0 -j ACCEPT
# Accept all encrypted VPN Client traffic in either direction on eth0
-A INPUT -i eth0 -p udp -s 0/0 --sport 500 -d 0/0 --dport 500 -j ACCEPT
-A OUTPUT -o eth0 -p udp -s 0/0 --sport 500 -d 0/0 --dport 500 -j ACCEPT
```

```
-A INPUT -i eth0 -p udp -s 0/0 --sport 4500 -d 0/0 --dport 4500 -j ACCEPT
-A OUTPUT -o eth0 -p udp -s 0/0 --sport 4500 -d 0/0 --dport 4500 -j ACCEPT
-A OUTPUT -o eth0 -p udp -s 0/0 --sport 1024: -d 0/0 --dport 29747 -j ACCEPT

# Block all other traffic in either direction on eth0
-A INPUT -i eth0 -j REJECT
-A OUTPUT -o eth0 -j REJECT
COMMIT
```

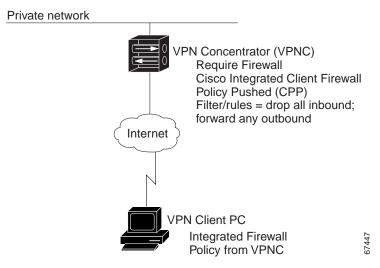
Firewall Configuration Scenarios

This section shows three sample firewall configurations. Each diagram shows the parameter settings in effect on the VPN Concentrator as well as the firewall product and policy in effect on the VPN Client.

Cisco Integrated Client

Figure 4-1 shows a typical configuration for Cisco Integrated Client, in which the policy (CPP) is pushed to the VPN Client. This policy blocks inbound traffic from the Internet while split tunneling is in use. Traffic from the private network is not blocked, however.

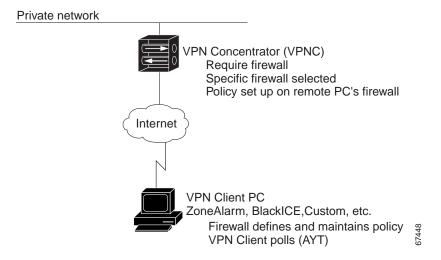
Figure 4-1 Cisco Integrated Client



Remote Firewall

Figure 4-2 shows a configuration in which the policy is set up on a personal firewall on the PC. In this case, Are You There (AYT) is the policy. The VPN Client polls the firewall every 30 seconds to ensure that it is still running and if it is not, the VPN Client terminates the session.

Figure 4-2 Remote Firewall Determines Policy



Client/Server Approach

Figure 4-3 shows a sample configuration for Zone Labs Integrity.

Figure 4-3 Client/Server—Integration With Zone Labs Integrity Server Integrity Server (IS) Gets User ID, Session ID, and Port from VPNC Provides connection information to VPNC Establishes policy; pushes policy to Integrity Agent (IA) Private network VPN Concentrator (VPNC) Knows address of IS Provides User ID/Session ID/Port to IS Sends User ID/Session ID/Port to VPN Client Internet VPN Client PC Integrity Agent (IA) IA installed and running VPNC and VPN Client negotiate VPNC passes User ID/Session ID/Port to Integrity Server **VPN Client** -- initializes IA with cached info --passes User ID/Session ID to IA IA connects with IS; gets firewall policy from IS IA starts enforcing policy VPN Client polls IA every 30 seconds If Firewall terminates, VPN connection dropped VPN Client uninitializes IA Caches policy

Defining a Filter and Rules to Use with Firewalls for CPP

When you want the VPN Concentrator to push the firewall policy to the VPN Client, you must first define the policy on the VPN Concentrator. To do this you need to create a filter and add rules to the filter on the public network. The VPN 3000 Concentrator provides a default filter you can use for CPP by selecting it from the menu. The name of this filter is "Firewall Filter for VPN Client (Default)". This filter allows all outbound traffic and drops all inbound traffic.

Firewall filters are session filters, rather than packet filters. This means that for an "allow all outbound/drop all inbound" rule, the CPP policy lets inbound responses come from outbound sessions *only* from IP protocols TCP, UDP, and ICMP. These protocols are the only protocols that are "stateful." Most administrators will want to use a rule that blocks all inbound traffic and either permits all outbound traffic or limits outbound traffic to specific TCP and UDP ports. For complete information on creating filters and adding rules in general, see *VPN 3000 Series Concentrator Reference Volume I:*Configuration, Configuration | Policy Management | Traffic Management.

Example 4-1 Creating a Filter for a Firewall Policy allowing the VPN Client to Act as a Web Server

This example shows step-by-step how to add a filter that allows outbound traffic to any protocol and to allow inbound traffic from HTTP but none of the other protocols. In this way, you can enable your VPN Client to become a Web server.

- Step 1 First, create a rule that allows inbound traffic only from HTTP. To do this, go to Configuration | Policy Management | Traffic Management | Rules.
- Step 2 Click Add
 - a. For the Rule Name, enter the name, such as FW-Allow incoming HTTP.
 - b. For Action, choose Forward.
 - **c.** For Protocol, choose **TCP**.
 - d. For TCP/UDP Destination Port, choose HTTP(80).
 - e. Click Add.
- Step 3 Next add a filter that drops all inbound traffic except from HTTP but forwards any outbound traffic while connected through a tunnel. To do this, under Traffic Management, click **Filters**.
 - a. Click the Add Filter box.
 - b. Enter the filter name, such as FW-Allow Incoming HTTP, and select the defaults for the remaining parameters.
 - c. Click Add, which brings up the Actions screen.
 - d. On this screen, highlight the rule you made in Step 2 and click **Add** to move it to the Current Rules in Filter column. Do the same for the Any Out (forward/out) rule.
 - e. Click Done.
- **Step 4** Save the configuration.

This filter now is available under Base Group and Groups for you to select for the CPP policy.

Configuring the VPN 3000 Concentrator to Enforce Firewall Usage on the VPN Client

This section shows how to configure the VPN Concentrator to require the VPN Client to enforce the use of a personal firewall on the VPN Client PC. On the VPN 3000 Concentrator side, you configure the Base Group or a specific group of users to enforce a personal firewall policy on the VPN Client side. Use the following general procedure.

- Step 1 To configure firewalls for the Base Group, choose Configuration | User Management | Base Group or to configure firewalls for a specific group, choose Configuration | User Management | Groups.
- Step 2 To add a firewall, do one of the following:
 - For the Base Group, choose the **Client FW** tab.
 - To create a new group for a firewall configuration, click Add Group and then click the Client FW tab.
 - To add a firewall to an existing group, highlight the group name, click Modify Group, and click the Client FW tab.
- Step 3 To require a firewall, under the Firewall Setting attribute, choose Firewall Required.
- Step 4 Under the Firewall attribute, choose a firewall from the Firewall pull-down menu. If the firewall you are using is not on the list, you must use **Custom**.
- Step 5 Choose the **Firewall Policy**: Policy defined by the remote firewall (AYT) or Policy pushed (CPP). (See the next section.)

For complete information, refer to *VPN 3000 Series Concentrator Reference Volume I: Configuration*, the section "User Management" or the VPN 3000 Concentrator Network Manager's online help.

Setting up Cisco Integrated Client Firewall (CIC) for CPP

- Step 1 Under Client FW tab on Firewall Setting, choose Firewall Required.
- Step 2 On the Firewall pull-down menu, choose Cisco Integrated Client Firewall.
- Step 3 On Firewall Policy, click **Policy Pushed** and select a filter that contains firewall policy rules. You can choose the default firewall filter or one that you have configured for a special purpose (see "Defining a Filter and Rules to Use with Firewalls for CPP").

Setting up a Client/Server Firewall —Zone Labs Integrity

- Step 1 Configure firewall policy on the Integrity Server (IS), following Zone Labs documentation.
- Step 2 On the VPN Concentrator, go to Configuration | System | Servers | Firewall Server. For the Zone Labs Integrity Server, enter the host name or IP address and the port number.

- Step 3 Under Configuration | User Management | Base Group or Groups | Client FW tab (see "Defining a Filter and Rules to Use with Firewalls for CPP"), configure the following:
 - a. Firewall Setting = Firewall Required
 - **b.** Firewall = **Zone Labs Integrity**
 - c. Firewall Policy = **Policy from Server**
- Step 4 Save the configuration.

Custom Vendor Codes

On the VPN 3000 Concentrator, you can configure a custom firewall. Table 4-1shows the custom vendor and product codes the VPN Client supports.

Table 4-1 Custom Vendor and Product codes

Vendor	Vendor Code	Products	Product Code
Cisco Systems	1	Cisco Integrated Client (CIC)	1
	5	Cisco Intrusion Prevention Security Agent	1
Zone Labs	2	Zone Alarm	1
		Zone AlarmPro	2
		Zone Labs Integrity	3
NetworkICE	3	BlackIce Defender/Agent	1
Sygate	4	Personal Firewall	1
		Personal Firewall Pro	2
		Security Agent	3

Obtaining Firewall Troubleshooting Information

This section describes two ways to obtain information about firewall negotiations: through the IPsec Log or a notification from the VPN Concentrator.

Examining the IPsec Log

One way to see what is happening during tunnel negotiation between the VPN Client and the VPN Concentrator is to examine messages in the IPsec Log on the VPN Client. You can use the Log Viewer application to do this (for information on using Log Viewer, refer to the *VPN Client User Guide for Windows*, Chapter 5). During tunnel negotiation, the VPN Client initiates the firewall exchange by sending the VPN Concentrator a list of firewalls installed and running on the PC, if any. The VPN Concentrator then sends messages indicating its firewall requirements to the VPN Client.

Following is an example of this exchange.

First, the request from the VPN Client to the VPN Concentrator:

```
36 16:44:39.250 02/28/03 Sev=Info/5
IKE/0x6300005D
Client sending a firewall request to concentrator

37 16:44:39.250 02/28/03 Sev=Info/5
IKE/0x6300005C
Firewall Policy: Product=Cisco Systems Integrated Client,
Capability= (Centralized Protection Policy).
```

Next, the responses from the VPN Concentrator:

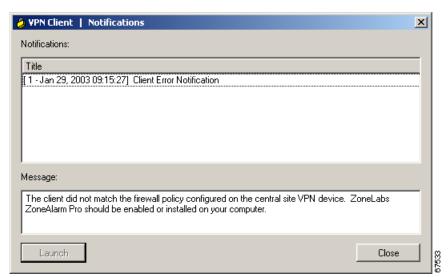
```
47 16:44:40.162 02/28/03 Sev=Info/5
IKE/0x6300005E
Client received a firewall reply from concentrator

48 16:44:40.162 02/28/03 Sev=Info/5
IKE/0x6300005C
Firewall Policy: Product=Cisco Systems Integrated Client, of Capability= (Centralized Protection Policy).
```

Notifications

If the VPN Client and VPN Concentrator firewall configurations do not match, the VPN Concentrator notifies the VPN Client when the VPN Client user attempts to connect. If the firewall configuration is required, the connection attempt fails; if the firewall configuration is optional, the tunnel comes up.

Figure 4-4 Firewall Mismatch Notification



Notifying Remote Users of a Client Update—All VPN Client Platforms

The security appliance or VPN 3000 Concentrator sends a separate notification message for each entry in a Client Update list. Therefore, your client update entries must not overlap. For example, the value Windows includes all Windows-based platforms, and the value WinNT includes Windows NT 4.0, Windows 2000, Windows XP, and Vista platforms. So you would not include both Windows and WinNT. To find out the client types and version information, click on the lock icon at the top left corner of the VPN Client main window and choose About VPN Client.

You can notify VPN Client users when it is time to update the VPN Client software on their remote systems. The notification can include a location containing the client update (the update does not happen automatically). Use the Client Update procedure at the VPN 3000 Concentrator to configure a client notification:

- Step 1 To enable Client Update, go to Configuration | System | Client Update and click Enable.
- Step 2 At the Configuration | System | Client Update | Enable screen, check **Enabled** (the default) and then click **Apply**.
- Step 3 On the Configuration | System | Client Update | screen, click Entries.
- Step 4 On the Entries screen, click Add. | The VPN Concentrator Manager, displays the Configuration | System | Client Update | Entries | Add or Modify screen.
- **Step 5** For Client Type, enter the operating systems to notify:
 - · Windows includes all Windows-based platforms
 - WinNT includes Windows NT 4.0, Windows 2000, Windows XP, and Windows Vista platforms
 - Linux
 - Solaris
 - · Mac OS X



The VPN 3000 Concentrator sends a separate notification message for each entry in a Client Update list. Therefore, your client update entries must not overlap. For example, the value **Windows** includes all Windows-based platforms, and the value WinNT includes Windows NT 4.0, Windows 2000, Windows XP, and Vista platforms. So you would not include both Windows and WinNT. To find out the client types and version information, click on the lock icon at the top left corner of the VPN Client main window and choose **About VPN Client**.

Step 6 In the URL field, enter the URL that contains the notification.

To activate the Launch button on the VPN Client Notification, the message must include the protocol HTTP or HTTPS and the server address of the site that contains the update. The message can also include the directory and filename of the update, for example, http://www.oz.org/upgrades/clientupdate. If you do not want to activate the Launch button for the remote user, you do not need to include a protocol in the message.

Step 7 In the Revisions field, enter a comma separated list of client revisions that do not need the update because they are already using the latest software. For example, the value 3.6.5 (Rel), 4.0 (Rel) identifies the releases that are compliant; all other VPN Clients need to upgrade.

Step 8 Click Add.

The Notification dialog box appears when the remote user first connects to the VPN device or when the user clicks the Notifications button on the Connection Status dialog box. When the notification pops up, on the VPN Client, click **Launch** on the Notification dialog box to open a default browser and access the URL containing the update.

Setting up Local LAN Access for the VPN Client

Remote users with Cable or DSL access from home might have home networks for sharing files and printers. You can configure local LAN access for remote users so that they can access resources on the LAN at the client side and still maintain the secure connection to the central site (through the IPsec tunnel).

Before you begin, you should carefully read the section on split tunneling in the *VPN 3000 Series Concentrator Reference Volume 1: Configuration*. See the section explaining Configuration | User Management | Groups | Add or Modify | IPsec tab.

Configuring local LAN access involves the following general steps:

- · Enabling local LAN access on the VPN Client
- Enabling local LAN access in specific groups on the VPN 3000 Concentrator
- Adding the accessible networks to a network list (or using the default network address).

Use the following procedure:

Step 1 On the VPN Client, enable the Allow Local LAN Access parameter.

When creating or modifying a connection entry, display the Transport tab and check **Allow Local LAN Access**.

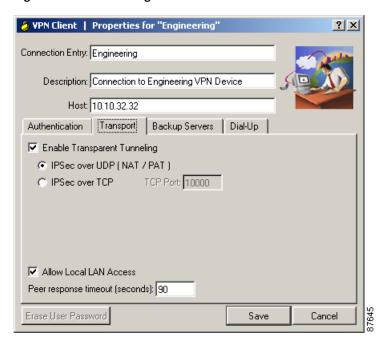


Figure 4-5 Setting the Allow Local LAN Access Parameter on the VPN Client

- Step 2 On the VPN 3000 Concentrator, either add a new group or modify an existing group as follows:
 - **a.** To configure local LAN access for a specific group, go to Configuration | User Management | Groups.
 - b. Choose either **Add** to add a new group or **Modify** to enable Local LAN for an existing group.
 - c. Go to the Client Config tab.
 - d. At the Split Tunneling Policy attribute, under Value, click the **Tunnel everything** radio button and then click **Allow the networks in list to bypass the tunnel**. This enables local LAN access on the VPN Client.
 - e. At the Split Tunneling Network List, under Value, choose the network list you have created for local LAN access, if any.

VPN Client Local LAN is the default and is assigned the address 0.0.0.0/0.0.0.0. This IP address allows access to all hosts on the client side LAN without regard to the network addressing configured on that network. Since this local LAN access is limited to only one local network, if you have multiple network cards in the client PC, you can access only the network in which the VPN Client has established the VPN connection.

For information on creating a network list, see *VPN 3000 Series Concentrator Reference Volume I: Configuration*, "Configuration | Policy Management | Traffic Management | Network Lists".



When the VPN Client is connected and configured for local LAN access, you cannot print or browse by name on the local LAN. When the VPN Client is disconnected, you can print or browse by name.

You can browse or print by IP Address. To print, you can change the properties for the network printer to use the IP Address instead of names. For example instead of the syntax \\sharename\printername, use \\x.x.x.\printername, where x.x.x.x is an IP address.

To print and browse by name, you can use an LMHOSTS file. To do this, add the IP addresses and local hostnames to a text file named LMHOSTS and place it on all your local PCs in the \Windows directory. The PC's TCP/IP stack then uses the IP address to hostname mapping in the LMHOSTS file to resolve the name when printing or browsing. This approach requires that all local hosts have a static IP address; or if you are using DHCP, you must configure local hosts to always get the same IP address.

Example LMHOSTS file:

192.168.1.100 MKPC 192.168.1.101 SBPC 192.168.1.101 LHPC

Configuring the VPN Concentrator for Client Backup Servers

This section shows how to configure a group on the VPN Concentrator to automatically push new backup server information to a VPN Client.

- **Step 1** On the VPN Concentrator, go to Configuration | User Management | Group.
- Step 2 To add a new group, click Add or to modify an existing group, highlight it in the box and click Modify.
- Step 3 Go to the Client Config tab.
- Step 4 For IPsec Backup Servers, select Use List Below from the drop-down menu.
- Step 5 Enter a list of up to 10 IPsec backup servers in high to low priority order.
- Step 6 Type each server address or name on a single line into the IPsec Backup Servers box.
- Step 7 Click Apply and then save the configuration.

Configuring NAT Traversal for the VPN Client

NAT Traversal (NAT-T) lets the VPN Concentrator establish IPsec tunnels with a VPN Client when there is a NAT device between them. It does this by encapsulating ESP traffic in UDP datagrams, which provides ESP with the port information that NAT devices require.

You can configure NAT-T globally on the VPN Concentrator, which then activates NAT-T for all groups configured on the VPN Concentrator.

Global Configuration

To configure NAT-T globally, follow these steps on the VPN Concentrator:

- Step 1 Go to Configuration | System | Tunneling Protocols | IPsec | NAT Transparency and check the **IPsec over** NAT-T check box.
- Step 2 Click Apply and then save the configuration.

Next configure the following parameters on the VPN Client.

- Step 1 If creating a new connection entry, click **New** under Connection Entries. If modifying an existing connection entry, highlight the entry and click **Modify**. In either case, a properties dialog box displays.
- Step 2 Open the **Transport** tab.
- Step 3 Check Enable Transparent Tunneling check box.
- Step 4 Click the **IPsec over UDP** (NAT/PAT) radio button.

Configuring Automatic Browser Configuration—Windows Only



This feature is supported only for Microsoft Internet Explorer web browser.

When a remote user connects to the VPN Concentrator (a secure gateway), the VPN Client can receive a web browser proxy setting from the VPN Concentrator and then change the web browser proxy configuration of the user to operate within the organization's environment. This setting is in effect only while the user is connected to the secure gateway. When the user disconnects, the VPN Client automatically changes the browser proxy of the PC to its original setting.

A network administrator configures this setting on the VPN Concentrator. Use the following procedure to configure the browser proxy setting for the VPN Client:

- Step 1 On the VPN Concentrator, go to Configuration | User Management | Base Group.
- Step 2 Click the VPN Client Config tab.
- Step 3 Scroll down to the Microsoft Client Parameters section.
- **Step 4** Edit the following sections:
 - a. Select the **IP Proxy Server Policy** method (following the instructions on the screen). Your choices are as follows. These choices are mutually exclusive.
 - Do not modify proxy settings—leaves the proxy setting unchanged
 - No proxy—disables the proxy setting in the VPN Client PC
 - Autodetect proxy—enables automatic detection of the proxy server setting in the VPN Client PC (but does not change it)
 - Use the proxy and server port configured in the IE Proxy Server box. If you choose this option, fill in the remaining boxes in this section of the Client Config tab. IE Proxy Server identity is required.
 - **b.** In the **IE Proxy Server** box, enter the name of the proxy server, a colon (:), and the port number for clients using Internet Explorer; for example, myproxy.mycompany.com:8080
 - c. In the **IE Proxy Serve Exception List**, enter the addresses or domains that are not to be accessed through a proxy server. This list corresponds to the Exceptions box in the Proxy Settings dialog box in Internet Explorer. You can enter wildcards; for example, www.*.org or 10.10.*
 - d. To allow local requests to bypass the proxy server, click Bypass Proxy Server for Local Addresses.

Step 5 Make sure you save the configuration.



The browser proxy feature in the VPN Client differs from Internet Explorer in the following ways: In Internet Explorer, auto detect policy and use proxy server/port are not mutually exclusive. The VPN Client supports only a single proxy server for all protocols, while for Internet Explorer, you can configure a proxy server for each protocol.

The VPN Client does not support the Internet Explorer option "Use automatic configuration script."

Configuring Entrust Entelligence for the VPN Client—Windows Only

This section explains how to set up a VPN Client to access Entrust Entelligence to obtain an Entrust identity certificate. It also provides information for using the VPN Client software with Entrust. For Entrust installation and configuration information, see your Entrust documentation—*Entrust Entelligence Quick Start Guide* or Entrust Entelligence online help.

Use the following procedure:

Step 1 Install Entrust Entelligence software on the remote user's PC.

You should install the Entrust Entelligence software before you install the VPN Client. The order is important when the VPN Client is using start before logon and Entrust SignOn at the same time. For information about what happens when both of these features are configured on the VPN Client, refer to VPN Client User Guide for Windows, Chapter 5.

Step 2 As part of Entust Entelligence installation, create a new Entrust profile, using the Create Entrust Profile Wizard.

To create an Entrust Entelligence profile, you need the following information:

- The Entrust Entelligence reference number
- The Entrust Entelligence authorization code
- The name of a directory for storing the profile
- A name for the profile
- · A password, following the rules set by the Entrust administrator
- Step 3 Optionally install Entrust SignOn, following the instructions in the Entrust documentation.
 - a. As part of Entrust SignOn installation, you see the Entrust Options dialog box. (See Figure 4-6.)
 - b. Make sure that you check **Always prompt me to confirm this login information**. Checking this box causes the Entrust SignOn login dialog box to pause and allow the VPN connection to come up before the remote user enters the NT logon information.

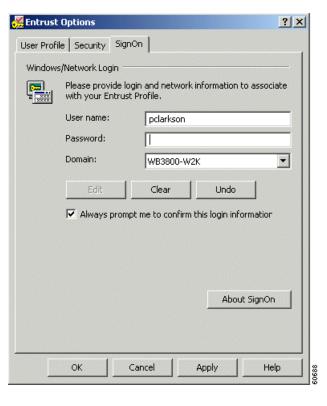


Figure 4-6 Entrust Options SignOn Tab

- **Step 4** After creating a profile, log out of Entrust Entelligence.
- Step 5 Install the VPN Client software.
- Step 6 Create a new connection entry that includes authenticating using an Entrust certificate. For instructions see section "Configuring an Entrust Certificate for Authentication," in Chapter 4 of VPN Client User Guide for Windows.



The VPN Client relies on an up-to-date Entrust DLL file. The name of this file is kmpapi32.dll. If you are using Entrust Entelligence version 5.1, the DLL file is up to date. If you have version 4.0 or 5.0 installed on the VPN Client system, then the DLL file is not up to date.

If "Entelligence Certificate (Entrust)" does not appear in the Certificate menu on the VPN Client, you probably do not have the latest version of the DLL file, which ships with the VPN Client software. To update the kmpapi32.dll file, copy it to the VPN Client system from the Release medium and place it in the Windows default system directory. For Windows NT, Windows 2000 and Windows XP systems, this directory is c:\WinNT\System32. For Windows 9x and Windows ME, the directory is \Windows\System.

Setting up the VPN Client for Authentication using Smart Cards—Windows Only

The VPN Client supports authentication via a certificate stored on a smart card. Once you create a connection entry and choose the certificate for authentication, the VPN Client user needs to insert the smart card into its reader. Once the VPN Client connection is initiated, the user is prompted to enter a PIN or passcode to obtain access to the smart card. The private key stays on the smart card and is never accessible without entering the PIN or passcode. Also, in most cases, there is a limit to how many times someone can try to enter the PIN or passcode after which there is a lock on the card.

Explaining how to configure VPN Client authentication for every smart card vendor is beyond the scope of this documentation. You must follow documentation from your smart card vendor to obtain this information.

In general:

- Step 1 Under Key Options, when you are performing web-based certificate enrollment, choose your smart card provider from the pull-down menu.
- Step 2 For Key usage choose **Signature** and verify that **Create new key set** is selected.
- Step 3 Install the certificate. The keys are generated on the smart card and a copy of the certificate is stored in the Microsoft store on your PC and listed on the VPN Client Certificates tab.
- **Step 4** Go to the Connection Entry > Modify dialog, and do the following:
 - a. Open the Authentication tab and check the Certificate Authentication radio button
 - b. Display the drop-down Name menu and click the smartcard certificate.

Now a VPN Client user can complete authentication only when the smart card is inserted in its reader that is plugged into the proper port on the PC and when the user enters the correct PIN or passcode.



With most vendors, when the smart card is not plugged in, the Certificates tab still displays the certificate. However when disconnected, e-token by Aladdin removes the certificate from the list. The certificate appears in the list only when the e-token is inserted and active.

Tear Down Tunnel When Smart Card Is Removed

When a smart card is removed from the system, the tunnel is automatically torn down. This causes the tunnel to immediately drop upon removal of the smart card from the system. This is an "always on" feature.

Notify User When a Smart Card Is Locked for Too Many Bad PINs

The VPN Client issues a log message when a smart card is blocked because too many incorrect PINs are entered. Under these circumstances, the connection eventually fails. The notification is a log message about the smart card being locked (CSCsb927).

Smart Card Password Reprompt for New Connections

Any time a new connection is made, the smart card requires the user to re-enter his or her credentials (password reprompt for new connections (uncache password)). The VPN Client does not allow connections to be re-established without the user re-entering the credentials to unlock the smart card.

To bypass this feature and retain the behavior found in earlier VPN Client releases, add an entry: BypassCardPinReset=1 in the vpnent.ini file. (CSCsb73937).

Smart Card Users Reauthenticating at Rekey

With VPN Client version 5.0.4 and later, the client prompts smart card users to reauthenticate when the VPN session is rekeyed. If the user does not reauthenticate, the VPN connection terminates. You can disable this behavior by configuring the CvpndSignHash parameter in the vpnclient.ini file. The following settings define the behavior of this parameter:

- CvpndSignHash=0 (default), or if the parameter missing—The authentication is not cached and the client prompts the user to reauthenticate during rekey.
- CvpndSignHash=1—The client caches the authentication. During rekey, the client *does not* prompt the user to reauthenticate

Configuring Mutual Authentication

This section contains information to help an administrator configure authentication on a VPN Client system and on the VPN Concentrator. These notes apply to all VPN Client platforms.

Configuring Mutual Group Authentication on the VPN Client System

Group Authentication is a method that uses pre-shared keys for mutual authentication. In this method, the VPN Client and the VPN central-site device use a group name and password to validate the connection. This is a symmetrical form of authentication since both sides use the same authentication method during their negotiations. Pre-shared authentication occurs in two stages.

During the first stage, the two sides exchange security parameters and create a secure channel. During the second stage, user authentication takes place. The VPN central-site device asks for username and password to verify that the remote user is a legitimate member of a group configured on the VPN central-site device.

Mutual group authentication is asymmetrical in that each side uses a different method to authenticate the other while establishing a secure tunnel to form the basis for group authentication. In this method, authentication happens in two stages. During the first stage, the VPN central-site device authenticates itself using public-key techniques (digital signature) and the two sides negotiate to establish a secure channel for communication. During the second stage, the actual authentication of the VPN Client user by the central-site VPN device takes place. since this approach does not use pre-shared keys for peer authentication, it provides greater security than group authentication alone as it is not vulnerable to a man-in-the-middle attack.

To use mutual group authentication, the remote user's VPN Client system must have a root certificate installed. If needed, you can install a root certificate automatically by placing it on the VPN Client system during installation. The certificate must be in a file named rootcert, with no extension and must be placed in the installation directory for the remote user's VPN Client system. For more information about loading a rootcert, see the installation instructions in the user guide for the remote user's platform

Configuring Mutual Authentication on the VPN Concentrator

The VPN Concentrator must use the same Certificate Authority (CA) as the VPN Client system for mutual authentication to take place. On the VPN Concentrator side, you must configure the following:

Step 1 Select an IKE proposal that allows HYBID mode authentication, such as those listed under "Command Line Switches" in Table 11-2 on page 11-11 of this manual. For example, in the VPN Concentrator, select HYBRID-AES256-SHA-RSA as the IKE proposal. For information on configuring IKE proposals, see VPN 3000 Series Concentrator Reference, Volume I, Configuration, the section on Configuration | Tunneling and Security | IPsec | IKE Proposals:

(http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_configuration_guide_chapter091 86a00801f1e36.html#1137591)



IKE proposals that include HYBRID mode authentication are not in the 4.1 Rel release of the VPN 3000 Concentrator. However, you can select them in the VPN 3000 Concentrator software for Release 4.6 and higher.

- Step 2 If the VPN Concentrator does not yet have an identity certificate, you need to enroll with the CA for the certificate. You can find information for doing so in VPN 3000 Series Concentrator Reference, Volume II, Administration and Monitoring, the section on Configuration Management:

 (http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_administration_guide_chapter09 186a00801f1dc5.html).
- Step 3 Configure an IPsec SA to use an identity certificate to be authenticated with the CA certificate of the VPN Client. You can find information in VPN 3000 Series Concentrator Reference, Volume I, Configuration, the section on Configuration | Policy Management | Traffic Management | Security Associations:

 (http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_configuration_guide_chapter091 86a00801f1dbb.html#1563342)
- Step 4 Configure a VPN Group on the VPN Concentrator to use the new IPsec SA from Step 3. For information on configuring VPN groups, see VPN 3000 Series Concentrator Reference, Volume I, Configuration, the section on Configuration | User Management | Groups, IPsec tab:

 (http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_configuration_guide_chapter091 86a00801f1df7.html#1907522.)



CHAPTER 5

Preconfiguring the VPN Client for Remote Users

This chapter explains how to prepare configurations for remote users and how to distribute them. This chapter includes the following sections:

- User Profiles
- · Creating a Global Profile
- Creating Connection Profiles

User Profiles

Groups of configuration parameters define the connection entries that remote users use to connect to a VPN central-site device. Together these parameters form files called profiles. There are two profiles: a global profile and an individual profile.

- A global profile sets rules for all remote users; it contains parameters for the VPN Client as a whole. The name of the global profile file is vpnclient.ini.
- Individual profiles contain the parameter settings for each connection entry and are unique to that connection entry. Individual profiles have a .pcf extension.

Profiles are created in two ways:

- 1. When an administrator or a remote user creates connection entries using the VPN Client graphical user interface (Windows and Macintosh only)
- 2. When you create profiles using a text editor

In the first case, the remote user is also creating a file that can be edited through a text editor. You can start with a profile file generated through the GUI and edit it. This approach lets you control some parameters that are not available in the VPN Client GUI application. For example, auto-initiation or dial-up wait for third-party dialers.

The default location for individual profiles is:

- For Windows platforms—C:\Program Files\Cisco Systems\VPN Client\Profiles.
- For the Linux, Solaris, and Mac OS X platforms—/etc/CiscoSystemsVPNClient/Profiles/

This chapter explains how to create and edit the vpnclient.ini and individual profiles. Both files use the same conventions.



The easiest way to create a profile for the Windows platforms is to run the VPN Client and use the VPN Client GUI to configure the parameters. When you have created a profile in this way, you can copy the .pcf file to a distribution disk for your remote users. This approach eliminates errors you might introduce by typing the parameters and the group password gets automatically converted to an encrypted format.

File Format for All Profile Files

The vpnclient.ini and .pcf files follow normal Windows.ini file format:

- Use a semicolon (;) to begin a comment.
- Place section names within brackets [section name]; they are not case sensitive.
- Use key names to set values for parameters; keyword = value. Keywords without values, or
 unspecified keywords, use VPN Client defaults. Keywords can be in any order and are not case
 sensitive, although using lower and uppercase makes them more readable.

Making a Parameter Read Only

To make a parameter read-only so that the client user cannot change it within the VPN Client applications, precede the parameter name with an exclamation mark (!). This controls what the user can do within the VPN Client applications only. You cannot prevent someone from editing the global or .pcf file and removing the read-only designator.

Creating a Global Profile

The name of the global profile is vpnclient.ini. This file is located in the following directories:

- For Windows platforms—C:\Program Files\Cisco Systems\VPN Client directory
- For the Linux, Solaris, and Mac OS X platforms—/etc/CiscoSystemsVPNClient/vpnclient.ini

These are the default locations created during installation.

Features Controlled by Global Profile

The vpnclient.ini file controls the following features on all VPN Client platforms:

- · Start before logon
- Automatically connect to the default connection entry (default profile) upon startup
- · Automatically disconnect upon log off
- · Control of logging services by class
- · Certificate enrollment
- · Identity of a proxy server for routing HTTP traffic
- Identity of an application to launch upon connect
- Missing group warning message
- · Logging levels for log classes

- RADIUS SDI extended authentication behavior
- GUI parameters—appearance and behavior of GUI applications

The vpnclient.ini file controls the following additional features in the Windows platform:

- · Location of the Entrust.ini file
- List of GINAs that are not compatible with the VPN Client
- Auto initiation
- · Setting of the Stateful Firewall option
- The method to use in adding suffixes to domain names on Windows 2000 and Windows XP platforms
- When working with a third-party dialer, time to wait after receiving an IP address before initiating an IKE tunnel
- Network proxy server for routing HTTP traffic
- · Application launching
- DNS suffixes
- Force Network Login, which forces a user on Windows NT, Windows 2000, or Windows XP to log
 out and log back in to the network without using cached credentials
- · Accessibility options setting
- Setting a default connection entry
- Connecting to a default connection entry

Sample vpnclient.ini file



Profiles for the VPN Client are interchangeable between platforms. Keywords that are specific to the Windows platform are ignored by other platforms.

This sample file shows what you might see if you open it with a text editor

[main] IncompatibleGinas=PALGina.dll,theirgina.dll RunAtLogon=0 EnableLog=1 DialerDisconnect=1 AutoInitiationEnable=1 AutoInitiationRetryInterval=1 AutoInitiationRetryLimit=50 AutoInitiationList=techsupport,admin [techsupport] Network=175.55.0.0 Mask=255.255.0.0 ConnectionEntry=ITsupport [admin] Network=176.55.0.0 Mask=255.255.0.0 ConnectionEntry=Administration Connectonopen=1 [LOG.IKE] LogLevel=1 [LOG.CM] LogLevel=1

```
[LOG.PPP]
LogLevel=2
[LOG.DIALER]
LogLevel=2
[LOG.CVPND]
LogLevel=1
[LOG.CERT]
LogLevel=0
[LOG.IPSEC]
LogLevel=3
[LOG.FIREWALL]
LogLevel=1
[LOG.CLI]
LogLevel=1
[CertEnrollment]
SubjectName=Alice Wonderland
Company=University of OZ
Department=International Relations
State=Massachusetts
Country=US
Email=AliceW@UOZ.com
CADomainName=CertsAreUs
CAHostAddress=10.10.10.10
CACertificate=CAU
[Application Launcher]
Enable=1
{\tt Command=c:\apps\apname.exe}
[NetLogin]
Force=1
Wait=10
DefaultMsg=For authorized users only
Separator=**************
WindowWidth=578
WindowHeight=367
WindowX=324
WindowY=112
VisibleTab=0
ConnectionAttribute=0
AdvancedView=1
DefaultConnectionEntry=ACME
MinimizeOnConnect=1
UseWindowSettings=1
ShowToolTips=1
ShowConnectHistory=1
AccessibilityOption=1
```

The rest of this section explains the parameters that can appear in the vpnclient.ini file, what they mean, and how to use them.

Global Profile Configuration Parameters

Table 5-1 lists all parameters, keywords, and values. It also includes the parameter name as used in the VPN Client GUI application if it exists, and where to configure it in the application.

Each parameter can be configured on all VPN Client platforms unless specified.

Table 5-1 vpnclient.ini File Parameters

.ini Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client GUI Configuration Location(s)
[main]	Required keyword to identify main section.	[main] Enter exactly as shown, as first entry in the file.	Does not appear in GUI
DialupWait	Specifies the number of seconds to wait between receiving an IP address from a third-party dialer such as General Packet Radio Services (GPRS) before initiating an IKE tunnel. This grants enough time for the connection to go through on the first attempt.	After the keyword and equal sign, enter the number of seconds to wait. For example: DialupWait=1 Default number = 0.	Does not appear in GUI
IncompatibleGinas (Windows-only)	Lists Graphical Identification and Authentication dynamic link libraries (GINA.DLLs) that are not compatible with Cisco's GINA. Adding a GINA to the list causes the VPN Client to leave the GINA alone during installation and use fallback mode. The VPN Client goes into fallback mode only if RunAtLogon = 1. Otherwise, the Client GINA is never installed. (See "Start Before Logon and GINAs—Windows Only".	After the keyword and equal sign, enter the name(s) of the GINAs, separated by commas. For example: IncompatibleGinas= PALgina.dll, Yourgina.dll, Theirgina.dll Do not enclose the name in quotes.	Does not appear in GUI
MissingGroupDialog	Controls the pop up window warning that occurs when a user tries to connect without setting the group name in a preshared connection.	0= (default) Do not show the warning message. 1=Show the warning message.	Does not appear in GUI
RunAtLogon (Windows-only)	Specifies whether to start the VPN Client connection before users log on to their Microsoft network. Available only for the Windows NT platform (Windows NT 4.0, Windows 2000 and Windows XP). This feature is sometimes known as the NT Logon feature.	0 = Disable (default) 1 = Enable	Options > Windows Logon Properties > Enable start before logon
EntrustIni= (Windows-only)	Locates the entrust.ini file if it is in a location that is different from the default.ini file. The default location is the base Windows system directory.	Complete pathname of location	Does not appear in GUI

Table 5-1 vpnclient.ini File Parameters (continued)

.ini Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client GUI Configuration Location(s)
DialerDisconnect= (Windows-only)	Determines whether to automatically disconnect upon logging off a Windows NT platform (Windows NT 4.0, Windows 2000 and Windows XP). Disabling this parameter lets the VPN connection remain when the user logs off, allowing that user to log back in without having to establish another connection.	0 = Disable 1 = Enable (default disconnect on logoff)	Options > Windows Logon Properties > Disconnect VPN connection when logging off

There are limitations to DialerDisconnect. For example, in the case of MS DUN, the RAS (PPP) connection might go down when the user logs off. For more information about this specific case, see the following URL:

EnableLog=	Determines whether to override log	0 = Disable	Log > Enable/Disable
	settings for the classes that use the logging services. By default, logging is turned on. This parameter lets a user disable logging without having to set the log levels to zero for each of the classes. By disabling logging you can improve the performance of the client system.	1 = Enable (default)	
StatefulFirewall= (Windows-only)	Determines whether the stateful firewall is always on. When enabled, the stateful firewall always on feature allows no inbound sessions from all networks, whether a VPN connection is in effect or not. Also, the firewall is active for both tunneled and nontunneled traffic.	0 = Disable (default) 1 = Enable	Options > Stateful Firewall (Always On)
StatefulFirewallAllow ICMP (Windows only)	Controls whether StatefulFirewall (Always On) allows ICMP traffic. Some DHCP Servers use ICMP pings to detect if the DHCP client PCs are up so that the lease can be revoked or retained.	0 = Disable (default) 1 = Enable	Does not appear in the GUI.
AutoInitiationEnable	Enables auto initiation, which is an automated method for establishing a wireless VPN connection in a LAN environment.	0 = Disable (default) 1 = Enable	Options > Automatic VPN Initiation

Table 5-1 vpnclient.ini File Parameters (continued)

.ini Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client GUI Configuration Location(s)
AutoInitiationRetry-Interval	Specifies the time to wait before retrying auto initiation after a connection attempt failure. The AutoInitiationRetryIntervalType parameter specifies whether this time is in minutes or seconds.	The default is 1 minute. The range is 1 to 10 minutes or 5 to 600 seconds.	Options > Automatic VPN Initiation
AutoInitiationRetry- IntervalType	Specifies whether the retry interval is displayed in minutes (the default) or seconds. The default is 0 (minutes).	0 = minutes (default) 1 = seconds	Options > Automatic VPN Initiation
AutoInitiationRetry- Limit	Identifies the number of consecutive connection failures before automatic initiation gives up and quits trying to connect.	1 to 1000 Default = 0 (no limit)	NA
AutoInitiationList	Identifies auto initiation-related section names within the vpnclient.ini file. The vpnclient.ini file can contain a maximum of 64 auto initiation list entries.	A list of section names separated by commas; for example: SJWLAN, RTPWLAN, CHWLAN	Does not appear in GUI
SetMTU (Non-Windows only, 4.8.x and higher)	Specifies the value to be used for the MTU while the VPN Client is connected. For comparison, Windows uses a default value of 1300.	After the keyword and equal sign, enter the MTU value to be used: • SetMTU=1356 (non-Windows default • SetMTU=1200 (suggested troubleshooting point)	Does not appear in GUI
CertificateKeyUsage (4.8.x)	Restricts the usage of certificates from all stores to only those with the following Certificate Key Usage parameters: Digital Signature or Non-repudiation. This keyword overrides all other certificate matching criteria, such as CertMatchDN, unless the CertMatchKU keyword is used in the profile.	CertificateKeyUsage=0 (Default) CertificateKeyUsage=1 (Digital Signature or Non-repudiation matching certificates only	Does not appear in GUI

Table 5-1 vpnclient.ini File Parameters (continued)

.ini Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client GUI Configuration Location(s)
[section name] (of an item in the AutoInitiationList)	Each section contains a network address, network mask, connection entry name, and a connect flag. The network and mask values identify a subnet. The connection entry identifies a connection profile (.pcf file). The connect flag specifies whether to auto initiate the connection.	Section name in brackets Network = IP address Mask = Subnet mask ConnectionEntry = name of a connection entry (profile) Connect = 1 or 0 0 = Do not auto initiate the connection 1 = Auto initiate the connection (the default) Example: [SJWLAN] Network=110.110.110.0 Mask=255.255.0.0 ConnectionEntry=SantaJuan WirelessLAN	Does not appear in GUI

Example of Automatic Initiation configuration for vpnclient.ini file:

[main]

AutoInitiationEnable = 1—Start automatic initiation.

autoInitiationList = autonet—identifies a section name in the list for automatic initiation.

 ${\tt AutoInitiationRetryInterval = 60-Try\ to\ connect\ every\ 60\ seconds.}$

AutoInitiationRetryIntervalType = 1—Set retry interval type to seconds.

AutoInitiationRetryLimit = 25—Try to connect 25 times. If connection attempts fail 25 times, stop trying to connect.

[autonet]—Start an entry in the automatic initiation list.

network = 192.168.0.0—Identify the IP address of the connection entry.

mask = 255.255.0.0—Specify the submask

connectionentry = flatirons—Specify the connection entry name s(.pcf file).

ConnectOnOpen	Automatically connects to the default user profile set in the DefaultConnectionEntry parameter	0 = Disable (the default) 1 = Enable	Main Menu > Options > Preferences > Enable connect on open
VAEnableAlt	Changes the method for initializing the virtual adapter from the standard method to an alternative method. If your users are experiencing difficulty in initializing the VA, try the alternate method.	0 = Use the alternate method for initializing the VA 1 = Use the standard method for initializing the VA (the default)	NA
AddDhcpRoute (Windows only)	Adds a route that bypasses all traffic going to the DHCP server. This is the normal behavior. However, if your users do not want the VPN Client to bypass all traffic going to the DHCP server because other services exist on the server, use this parameter to change the default behavior of the software.	0 = Do not add a route to bypass the DHCP server 1 = Add a route to bypass the DHCP server (default)	

For each class that follows, use the LogLevel= parameter to set the logging level to a value from 0 through 15.

Table 5-1 vpnclient.ini File Parameters (continued)

.ini Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client GUI Configuration Location(s)
[LOG.IKE]	Identifies the Internet Key Exchange class for setting the logging level.	[LOG. IKE] Enter exactly as shown.	Log > Settings
[LOG.CM]	Identifies the Connection Manager class for setting the logging level.	[LOG.CM] Enter exactly as shown.	Log > Settings
[LOG.XAUTH]	Identifies the Extend authorization class for setting the logging level.	[LOG.XAUTH] Enter exactly as shown.	Log > Settings
[LOG.PPP] (Windows-only)	Identifies the PPP class for setting the logging level.	[LOG. PPP] Enter exactly as shown.	Log > Settings
[LOG.CVPND]	Identifies the Cisco VPN Daemon class for setting the logging level.	[LOG.CVPND] Enter exactly as shown.	Log > Settings
[LOG.CERT]	Identifies the Certificate Management class for setting the logging level.	[LOG.CERT] Enter exactly as shown.	Log > Settings
[LOG.IPSEC]	Identifies the IPsec module class for setting the logging level.	[LOG. IPSEC] Enter exactly as shown.	Log > Settings
[LOG.FIREWALL] (Windows-only)	Identifies the FWAPI class for setting the logging level.	[LOG.FIREWALL] Enter exactly as shown	Log > Settings
[LOG.CLI]	Identifies the Command-Line Interface class for setting the logging level.	[LOG.CLI] Enter exactly as shown	Log > Settings
[LOG.GUI]	Identifies the Graphical User Interface class for setting the logging level.	[LOG.GUI] Enter exactly as shown	Log > Settings
LogLevel=	Determines the log level for individual classes that use logging services. By default, the log level for all classes is Low. You can use this parameter to override the default setting for the preceding [LOG] parameters.	The VPN Client supports log levels from 1 (lowest) to 15 (highest). Default = 1 To set logging levels, you must first enable logging: EnableLog=1.	Log > Settings
[CertEnrollment]	Required keyword to identify the Certificate Enrollment section.	[CertEnrollment] Enter exactly as shown.	Does not appear in GUI
SubjectName=	Identifies the username associated with this certificate.	Maximu"""m of 519 alphanumeric characters.	Certificates > Enroll Certificate Enrollment form
Company=	Identifies the company or organization of the certificate owner.	Maximum of 129 alphanumeric characters.	Certificates > Enroll Certificate Enrollment form

Table 5-1 vpnclient.ini File Parameters (continued)

.ini Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client GUI Configuration Location(s)
Department=	Identifies the department or organizational unit of the certificate owner. If matching by IPsec group in a VPN 3000 Concentrator, must match the group name in the configuration.	Maximum of 129 alphanumeric characters.	Certificates > Enroll Certificate Enrollment form
State=	Identifies the state or province of the certificate owner.	Maximum of 129 alphanumeric characters.	Certificates > Enroll Certificate Enrollment form
Country=	Identifies the two-letter code identifying the country of this certificate owner.	Maximum of 2 alphanumeric characters.	Certificates > Enroll Certificate Enrollment form
Email=	Identifies the certificate owner's email address.	Maximum of 129 alphanumeric characters.	Certificates > Enroll Certificate Enrollment form
IPAddress	Identifies the IP address of the system of the certificate owner.	Internet address in dotted decimal notation.	Certificates > Enroll Certificate Enrollment form
Domain	Identifies the fully qualified domain name of the host that is serving the certificate owner.	Maximum of 129 alphanumeric characters.	Certificates > Enroll Certificate Enrollment form
CADomainName=	Identifies the domain name that the certificate authority belongs to; for network enrollment.	Maximum of 129 alphanumeric characters.	Certificates > Enroll Certificate Enrollment form
CAHostAddress=	Identifies the IP address or hostname of the certificate authority.	Internet hostname or IP address in dotted decimal notation. Maximum of 129 alphanumeric characters.	Certificates > Enroll Certificate Enrollment form
CACertificate=	Identifies the name of the self-signed certificate issued by the certificate authority.	Maximum of 519 alphanumeric characters. Note: The VPNClient GUI ignores a read-only setting on this parameter.	Certificates > Enroll Certificate Enrollment form
NetworkProxy= (Windows-only)	Identifies a proxy server you can use to route HTTP traffic. Using a network proxy can help prevent intrusions into your private network.	IP address in dotted decimal notation or domain name. Maximum of 519 alphanumeric characters. The proxy setting sometimes has a port associated with it. Example:10.10.10.10:8080	Does not appear in GUI

Table 5-1 vpnclient.ini File Parameters (continued)

.ini Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client GUI Configuration Location(s)
[ApplicationLauncher] (Windows-only)	(No VPN Client field) Required keyword to identify Application Launcher section.	[ApplicationLauncher] Enter exactly as shown, as first entry in the section.	Does not appear in GUI
Enable= (Windows-only)	Use this parameter to allow VPN Client users to launch an application when connecting to the private network.	0 = Disabled (default) 1 = Enabled Disabled means no launching.	Options> Application Launcher
Command= (Windows-only)	The name of the application to be launched. This variable includes the pathname to the command, and the name of the command complete with arguments.	command string Maximum 512 alphanumeric characters. Example: c:\auth\swtoken.exe.	Options> Application Launcher> Application
[DNS] (Windows-only)	(No VPN Client field) Required keyword to identify DNS section.	[DNS] Enter exactly as shown, as first entry in the section.	Does not appear in GUI.
AppendOriginalSuffix= (Windows-only)	Determines the way the VPN Client treats suffixes to domain names. See "DNS Suffixes and the VPN Client—Windows Vista, Windows XP, and Windows 2000 Only", following this table.	0 = do nothing 1= append the primary DNS suffix to the suffix that the VPN Concentrator supplies. This is the default value. 2= append the primary and connection-specific DNS suffixes to the suffix that the VPN Concentrator supplies.	Does not appear in GUI.
[RadiusSDI]	Required keyword to identify the RADIUS SDI extended authentication (XAuth) section. Configure this section to enable a VPN Client to handle Radius SDI authentication the same as native SDI authentication, which makes authentication easier for VPN Client users to authenticate using SDI.	Enter exactly as shown.	Does not appear in GUI.
EnableDNSRedirection (Windows only, 4.8.01.x and higher)	Allows modification of DNS redirection default behavior.	After the keyword and equal sign, enter either 0 or 1; for example: EnableDNSRedirection=0 (default for split-tunneling) EnableDNSRedirection=1 (default for tunnel all)	Does not appear in GUI

Table 5-1 vpnclient.ini File Parameters (continued)

.ini Pa	rameter (Keyword)	VPN Client Parameter Description	Values	VPN Client GUI Configuration Location(s)
Questi	ionSubStr	Uniquely identifies question-type RADIUS SDI Xauth prompts.	Enter text up to 32 bytes in length. The default text is a question mark. Example:	The question appears in the GUI during extended authentication. It is followed by a
			"Are you prepared to have the system generate your PIN? (y/n):"	Response field.
NewPir	nSubStr	Uniquely identifies new PIN RADIUS SDI Xauth prompts.	Enter text up to 32 bytes in length. Default text is "new PIN." Example:	Appears in the GUI during extended authentication.
			"Enter a new PIN of 4 to 8 digits."	
NewPas	sscodeSubStr	Uniquely identifies new passcode RADIUS Xauth prompts.	Enter text up to 32 bytes in length. Default text is "new passcode."	Appears in the GUI during extended authentication.
			Example:	
			"PIN accepted.	
			Wait for the token code to change, then enter the new passcode"	
[Netlo	ogin] ows-only	Identifies the Force Network Login section of the vpnclient.ini file. This feature forces a user on Windows NT, Windows 2000, and Windows XP to log out and log back in to the network without using cached credentials.	Enter exactly as shown; this is required as part of the feature.	Does not appear in the GUI.
Note	http://support.micros	ng via dialup (RAS), you should add the soft.com/default.aspx?scid=kb;en-us;Q drop when the user gets logged off.		
Force (windo	ows-only)	Specifies what action to take for the Force Network Login feature. This parameter is required for this feature.	0 = (default) Do not force the user to log out and log in. 1 = Force user to log out when the Wait time is reached unless an option is selected. 2 = Disconnect VPN session upon reaching the Wait time unless an option is selected. 3 = Wait for the user to select Connect or Disconnect.	Does not appear in the GUI.

Table 5-1 vpnclient.ini File Parameters (continued)

.ini Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client GUI Configuration Location(s)
Wait (windows-only)	Determines the number of seconds to wait before performing an action specified by the Force parameter. This parameter is optional.	x number of seconds. The default is 5 seconds.	Does not appear in the GUI.
DefaultMsg (windows-only)	Specifies a message to display before performing the action specified by the Force parameter. Message can vary according to setting of Force. This parameter is optional.	Ascii text up to 1023 bytes. Default message = You will soon be disconnected.	Does not appear in the GUI.
Separator (windows-only)	Specifies the separator text that separates banner text from the message. If no banner exists, the separator is not displayed. This parameter is optional.	Ascii text up to 511 bytes. Default separator =	Does not appear in the GUI.
[GUI]	Required keyword to identify the section of the file that lets you control features of the Graphical User Interface application.	[GUI] Enter exactly as shown, as first entry in the section.	Does not appear in the GUI.
DefaultConnectionEntry	Specifies the name of the connection entry for the VPN Client to use to initiate a connection, unless otherwise indicated.	ConnectionEntryName	Connection Entries > Add/Modify > Set as default entry.
WindowWidth	Controls the width of the window.	Default = 578 pixels	Manual control
WindowHeight	Controls the height of the window.	Default = 367 pixels	Manual control
WindowX	Controls the X coordinate of the window.	0 to 1024 pixels Default = 324	Where the window appears horizontally relative to your monitor's screen
WindowY	Controls the Y coordinate of the window.	0 to 768 pixels Default = 112	Where the window appears vertically relative to your monitor's screen
VisibleTab	Tracks which tab is currently visible in the advanced mode main dialog; an index.	Connection Entries Certificates Log	VPN Client main dialog
ConnectionAttibute	Indicates the current setting for the status bar display. The status bar is the line area at the bottom of the dialog that shows the state of the connection (connect/not connected), if connected, the name of the connection entry on the left and what the status is on the right.	If you click on the arrow on the right end of the status bar, the right part of the status bar changes. This value records the current display selection.	VPN Client main dialog > status bar

Table 5-1 vpnclient.ini File Parameters (continued)

.ini Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client GUI Configuration Location(s)
AdvancedView	Toggles between Advanced and Simple modes of operation.	Simple Mode = 0 Advanced Mode = 1 (default)	Main menu > Options menu > Advanced/ Simple Mode
MinimizeOnConnect	Controls whether to minimize to a system tray icon upon connection to a VPN central-site device.	0 = Do not minimize 1 = Do minimize (default)	Main menu > Options > Preferences > Hide upon connect
UseWindowSettings	Controls whether to save windows settings.	0 = No 1 = Yes (default)	Main menu > Options > Preferences > Save window settings
ShowTooltips	Controls whether to display the tool tips.	0 = No 1 = Yes (default)	Main menu > Options > Preferences > Enable tooltips
ShowConnectHistory	Controls whether to display the connection history dialog during connection negotiation.	0 = No (default) 1 = Yes	Main menu > Options > Preferences > Enable Connection History Display
AccessibilityOption	Controls whether to activate 508 accessibility options (Windows only)	0 = No (default) 1 = Yes	Main menu > Options > Preferences > Enable accessibility options
ShowConnectionTab ShowCertificatesTab ShowLogTab	Allows tabs to be hidden on GUI.	After keyword and equal sign, enter either 0 or 1; for example:	Does not appear in GUI.
(GUI clients only, 4.8.x)		• ShowConnectionTab=1 (default)	
		• ShowConnectionTab=0	
ShowCertTabDelete Show CertTabChangePasswd (GUI clients only, 4.8.x)	Allows these features to be hidden from the GUI and prevents userf from accidentally deleting certificates or	After the keyword and equal sign, enter either 0 or 1; for example:	Does not appear in GUI.
	changing their certificate password.	ShowCertTabDelete=1 (default)	
		ShowCertTabDelete=0 (hides certificate delete option)	

Connecting with Digital Certificates

Before you create a VPN Client connection entry using a digital certificate, you must have already enrolled in a Public Key Infrastructure (PKI), have received approval from the Certificate Authority (CA), and have one or more certificates installed on the VPN Client system. If this is not the case, then you need to obtain a digital certificate. You can obtain one by enrolling with a PKI directly using the Certificate Manager feature, or you can obtain an Entrust profile through Entrust Entelligence. Currently, we have tested the following PKIs:

UniCERT from Baltimore Technologies (www.baltimoretechnologies.com)

- Entrust PKITM 5.0 from Entrust Technologies (www.entrust.com)
- Versign (www.verisign.com)
- RSA KEON 5.7 and 6.0
- Microsoft Certificate Services 2.0
- Cisco Certificate Store

The Web sites listed in parentheses in this list contain information about the digital certificates that each PKI provides.

Certificate Distinguished Name Matching

For Windows and Linux platforms, the Profile Keyword: CertMatchDN parameter specifies the wildcard string to match and selects a particular certificate by its Distinguished Name, in the given certificate store, during a connection attempt. If the wildcard string matches multiple certificates, the first certificate that satisfies the wildcard string is chosen. The value of this parameter is a pseudo-regular expression, the format of which is exactly identical to that of the VerifyCertDN profile keyword.

Valid keywords for the wildcard string are:

- "CN" SubjectCommonName
- "SN" SubjectSurName
- "GN" SubjectGivenName
- "N" SubjectUnstructName
- "I" SubjectInitials
- "GENQ" SubjectGenQualifier
- · "DNQ" SubjectDnQualifier
- "C" SubjectCountry
- · "L" SubjectCity
- "SP" SubjectState
- "ST" SubjectState
- "O" SubjectCompany
- "OU" SubjectDept
- "T" SubjectTitle
- "EA" SubjectEmailAddr
- "ISSUER-CN" IssuerCommonName
- "ISSUER-SN" IssuerSurName
- "ISSUER-GN" IssuerGivenName
- "ISSUER-N" IssuerUnstructName
- · "ISSUER-I" IssuerInitials
- · "ISSUER-GENQ" IssuerGenQualifier
- · "ISSUER-DNQ" IssuerDnQualifier

- "ISSUER-C" IssuerCountry
- "ISSUER-L" IssuerCity
- "ISSUER-SP" IssuerState
- "ISSUER-ST" IssuerState
- "ISSUER-O" IssuerCompany
- "ISSUER-OU" IssuerDept
- "ISSUER-T" IssuerTitle
- "ISSUER-EA" IssuerEmailAddr

Example:

```
CertMatchDN=CN="ID Cert",OU*"Cisco",ISSUER-CN!="Entrust",ISSUER-OU!*"wonderland" CN="ID Cert"--Specifies an exact match on the CN.

OU*"Cisco"--Specifies any OU that contains the string "Cisco".

ISSUER-CN!"Entrust"--Specifies that the Issuer CN must not equal "Entrust".

ISSUER-OU!*"wonderland"--Specifies that the Issuer OU must not contain "wonderland".
```

Certificate Key Usage

For Windows, Linux, and Mac platforms, the global parameter vpnclient.ini [Main] keyword: CertificateKeyUsage restricts the usage of Certificates from all stores to only those with the Certificate Key Usage parameters: Digital Signature or Non-Repudiation.

If the "CertificateKeyUsage=1" when the client is launched, only Certificates with the proper key usage are displayed under the Certificates tab. In addition, profiles configured to use Certificates that do not have the proper key usage receive an error that the Certificate cannot be found.

The default for this keyword is "CertificateKeyUsage=0", which allows all available Certificates to be selected and used.

This keyword overrides all other Certificate matching criteria, such as CertMatchDN.

Certificate Key Usage Matching

For Windows and Linux platforms, the Certificate Key Usage Matching feature allows the profile selection of Certificates based on the Key Usage as well as the DN and Extended Key Usage fields. This global parameter restricts the use of Certificates from all stores to only those with the following Certificate Key Usage parameters: Digital Signature or Non-Repudiation.

If CertificateKeyUsage=1 when the Client is launched, only Certificates with the proper key usage are displayed under the Certificates tab. Profiles that do not have the proper key usage receive an error indicating that the Certificate cannot be found.

The default for this keyword is CertificateKeyUsage=0, which allows all available Certificates to be selected and used. This keyword, CertificateKeyUsage takes precedence over all other Certificate matching criteria, such as CertMatchDN, unless it is specifically changed using the CertMatchKU keyword in the profile being used.

The Profile Keyword: CertMatchKU overrides the vpnclient.ini keyword "CertificateKeyUsage" (CSCsc32638).

For example:

CertMatchKU=0,3,4,5

```
DIGITAL_SIGNATURE 8
NON_REPUDIATION 7
KEY_ENCIPHERMENT 6
DATA_ENCIPHERMENT 5
KEY_AGREEMENT 4
KEY_CERT_SIGN 3
CRL_SIGN 2
ENCIPHER_ONLY 1
DECIPHER_ONLY 0
```

If the Certificate matches any of the usages in the CertMatchKU field, it passes on to the next criterion. Otherwise, the Certificate is not selected.

If two Certificates, identical except for Key Usage, are available to the following profile, only the one with Non-Repudiation is chosen.

```
[Main]
Host=1.2.3.4
AuthType=3
CertStore=2
CertName=myMultipleCerts
CertMatchKU=7
!CertSubjectName=
!CertSerialHash=
```

Certificate Extended Key Usage Matching

The profile keywordparameter CertMatchEKU specifies the list of extended Key Usage fields that the VPN Client should honor. When this profile keyword is specified, during a connection attempt the VPN Client looks only at those certs (irrespective of certificate store) whose Extended Key Usage fields match those that are specified by the profile keyword. That is, when this profile keyword is specified, for any given cert, at least one of the Extended Key Usage fields specified in the profile keyword must be prresent in the certificate's Extended key Usage field.

This keyword applies to connection attempts only and not to any other certificate-related operation (such as listing certs, viewing certs, and so on). This keyword applies to all forms of certificate selection (such as CertSeriaHash, CertMatchDN, CertSubjectName, or CertName). The value of this keyword is a comma-separated list of Extended Key Usage OID strings. Custom Extended Key Usage strings must be of the form 1.3.6.1.5.5.7.3.n, where n can be any number.

For example:

```
CertMatchEKU=1.3.6.1.5.5.7.3.2,1.3.6.1.5.5.7.3.1 where:

1.3.6.1.5.5.7.3.2 = Client authentication

1.3.6.1.5.5.7.3.1 = Server Authentication
```

Certificate Fall Through

This behavior is implicit and does not have any profile keyword associated with it. For a given connection attempt, you can select a certificate using one or more of the following keywords (given in order of precedence):

- 1. CertSerialHash
- 2. CertMatchDN

- 3. CertSubjectName
- 4. CertName

If the VPN Client cannot find a cert in the given cert store using all of the Certificate keywords noted above, the connection attempt fails.

The following is a sample profile:

```
[Main]
Host=10.10.10.10
AuthType=3
CertStore=2
!UserName=
!UserPassword=
CertMatchDN=issuer-ou*"vpn group",ea*"Cisco.com"
!CertSerialHash=
```

This profile matches only certificates that have a Key Usage of "Non-Repudiation" and have either Client or Server Authentication in the Extended Key Usage. The Issuer-ou field must contain "vpn group", and the email address for the user Certificate must contain "cisco.com" (case insensitive).

In the Windows environment (the VPN Clients for Linux and Mac do not support smart cards), the preceding scenario allows a common workstation to connect users based on their smart card certificates. A user could walk up, insert the smart card, and press connect. This generic profile would find the proper certificate on the card (without restarting the client or modifying the profile) and prompt the user for his or her Certificate password, username, and password. The secure gateway could also be configured to connect without a username and rely entirely upon the Certificates for authentication.



The use of the "!" character in the profile prevents the previous user's information from being retained between connections.

Certificate Matching matches the first available Certificate that matches the rules set up for Certificate Matching, regardless of validity, causing the connection to fail. To prevent expired certificates from being selected when valid ones are available, the Windows VPN Client now ignores invalid or expired Certificates from the Certificate Store. (CSCsd38373, CSCsd38360).

Important Note about Using CertSerialHash

When using DN or other match criteria to find a certificate such as the example below:

```
CertMatchDN=CN*"User"
!CertSerialHash=
```

the Client cannot update the serial hash value because the exclamation point (!) in front of the key word makes CertSerialHash a read-only field. Without the correct serial hash, the Client cannot create a watch timer to verify the existence of the Smartcard.

Without "!CertSerialHash=", the Client updates the cert hash with the certificate in the store and adds following line into the profile:

```
CertSerialHash=...03CF...
```

If a serial hash value already exists in the profile, such as "CertSerialHash=0102...xyz", and if you use a different Smartcard with a different certificate that matches the DN, the Smartcard watch also starts, but IPsec updates the serial hash value of the CertSerialHash parameter to that of the certificate being used.



It's essential *not* to use '!' in front of "CertSerialHash=" in this context, because you must allow the VPN Client to update the serial hash value to the intended certificate.

Creating and Using a Default User Profile

You can configure a default user profile, which is the same as the default connection entry capability in the VPN Client GUI (see VPN Client User Guide for Windows, Chapter 4, "Setting a Default Connection Entry" or VPN Client User Guide for Mac OS X, Chapter 5, "Connecting to a Default Connection Entry." The parameter DefaultConnectionEntry in the VPN Client .ini file contains the name of the default user profile. Then you can use the Connect on Open feature to configure the VPN Client to connect to the default user profile when it connects to a secure gateway. To activate this configuration, using the parameters in the vpnclient.ini file, use the following procedure:

- Step 1 Specify the name of a default connection entry in the DefaultConnectionEntry parameter; for example, DefaultConnectionEntry=myprofile.
- Step 2 Enable the ConnectOnOpen parameter (ConnectOnOpen=1).

DNS Suffixes and the VPN Client—Windows Vista, Windows XP, and Windows 2000 Only

When a command or program such as **ping server123** passes a hostname without a suffix to a Windows Vista, Windows XP or Windows 2000 platform, the Windows operating system must convert the name into a fully-qualified domain name (FQDN). The Windows operating system has two methods for adding suffixes to domain names: Method 1 and Method 2. This section describes these two methods.

Method 1—Primary and Connection-Specific DNS Suffixes

A primary DNS suffix is global across all adapters. A connection-specific DNS suffix is only for a specific connection (adapter), so that each connection can have a different DNS suffix.

Identifying a Primary DNS Suffix

A primary suffix comes from the computer name. To find or assign a primary DNS suffix, use the following procedure according to your operating system:

On Windows 2000

- Step 1 On a Windows 2000 desktop, right click the **My Computer** icon, and select **Properties** from the menu. The System Properties dialog displays.
- Step 2 Open the **Network Identification** tab.

The entry next to Full Computer Name identifies the computer's name and DNS suffix on this screen, for example, SILVER-W2KP.tango.dance.com. The part after the first dot is the primary DNS suffix, in this example: tango.dance.com.

Step 3 To change the primary DNS suffix, click **Properties** on the Network Identification tab.

The Identification Changes dialog displays.

Step 4 Click More....

This action displays the DNS Suffix and Net BIOS Computer Name dialog. The Primary DNS suffix of this computer entry identifies the primary suffix. You can edit this entry.

On Windows XP

Step 1 Right click My Computer, and select Properties from the menu.

The System Properties dialog displays.

Step 2 Open the Computer Name tab.

The entry next to Full Computer Name identifies the computer's name and DNS suffix on this screen (for example, SILVER-W2KP.tango.dance.com). The part after the first dot is the primary DNS suffix (in this example: tango.dance.com).

Step 3 To change the primary DNS suffix, click **Change** on the Computer Name tab.

The Computer Name Changes dialog displays.

Step 4 Click More....

This action displays the DNS Suffix and Net BIOS Computer Name dialog. The Primary DNS suffix of this computer entry identifies the primary suffix. You can edit this entry.

Identifying a Connection-Specific DNS Suffix

You can identify a connection-specific DNS suffix in one of two ways.

1. The connection-specific DNS value is listed as the DNS suffix for the selected connection on the Advanced TCP/IP Settings dialog.



The following instructions are for a Windows 2000 platform. There may be slight variations on a Windows XP platform.

To display the Advanced TCP/IP Settings dialog, use the following procedure:

- Step 1 Right click the My Network Places icon to display the Properties dialog, which lists your connections.
- Step 2 Double-click on a connection (for example, **local**) to display its Properties dialog. The connection uses the checked components, such as those shown in Figure 5-1, which shows components of a connection named Local Area Connection.

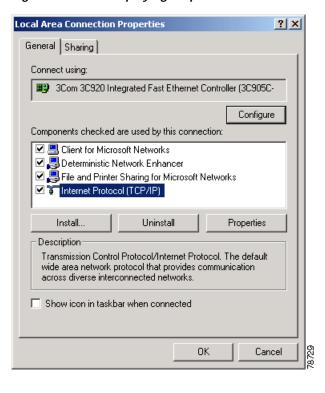


Figure 5-1 Displaying Properties for a Connection

- Step 3 Double-click Internet Protocol (TCP/IP) to reveal its properties.
- Step 4 Select Advanced.
- Step 5 Display the **DNS** tab and look at DNS suffix for this connection box. If the box is empty, you can have it assigned by the DHCP Server.
 - a. To identify the connection-specific suffix assigned by the DHCP Server, use the **ipconfig /all** command (Alternative 2, below) and for the DNS Server address.
 - 2. The connection-specific DNS value is listed in the output from the **ipconfig /all** command, executed at the command-line prompt. Look under Windows 2000 IP Configuration for DNS Suffix Search List. Under Ethernet Adapter Connection Name, look for Connection-specific DNS Suffix.

Method 2—User Supplied DNS Suffix

For this method, you can provide specific suffixes. You can view and change suffixes in the DNS tab of the connection properties page. The Append these DNS suffixes (in order) edit box supplies the name that you can edit. The values you provide here are global to all adapters.

VPN Client Behavior

When the VPN Client establishes a VPN tunnel to the VPN central device (for example, the VPN 3000 Concentrator), the VPN Client uses Method 2 without regard for the method that the Windows platform uses. If the Windows platform is using Method 2, the VPN Client appends the suffix provided by the VPN central device. This is the default behavior and works correctly with no problem.

However if Windows is using Method 1, the VPN Client does not append the primary or connection-specific suffix. To fix this problem, you can set the AppendOriginalSuffix option in the vpnclient.ini file. In Table 5-1, the [DNS] section contains this option:

[DNS]

AppendOriginalSuffix=1:

In this case, the VPN Client appends the primary DNS suffix to the suffix provided by the VPN Concentrator. While the tunnel is established, Windows has two suffixes: one provided by the VPN Concentrator and the primary DNS suffix.

AppendOriginalSuffix=2:

In this case, the VPN Client appends the primary and connection-specific DNS suffixes to the suffix provided by the VPN Concentrator. While the tunnel is established, Windows has three suffixes: one provided by the VPN Concentrator, the primary DNS suffix, and the connection-specific DNS suffix.



If Windows is using Method 2, adding these values to the vpnclient.ini file has no effect.

The VPN Client sets these values every time a tunnel is established and then restores the original configuration when tearing down the tunnel.

Setting Up RADIUS SDI Extended Authentication

You can configure the VPN Client to handle RADIUS SDI authentication the same way it handles "native" SDI authentication, which is more seamless and easier to use. With this configuration, users do not have to deal with the RSA SecurID software interface; the VPN Client software directly interfaces with the RSA SecureID software for the user.

To enable intelligent handling of RADIUS SDI authentication, you must configure one profile (.pcf) parameter and possibly three global (vpnclient.ini) parameters:

- In the vpnclient.ini file, enter the following information. (For complete information on these parameters, see Table 5-1.)
 - RadiusSDI—identifies the configuration section for RADIUS SDI
 - A question sub-string to identify question prompts (e.g. "?")
 - A new PIN sub-string to identify prompts for a new PIN
 - A new passcode sub-string to identify prompts for a new passcode
- In the profile (connection entry) file under the Main section, enter the parameter "RadiusSDI = 1". (See Table 5-2.)

Now when the request comes in to the VPN Client, the software identifies it as a RADIUS SDI extended authentication request and knows how to process the request.

Creating Connection Profiles

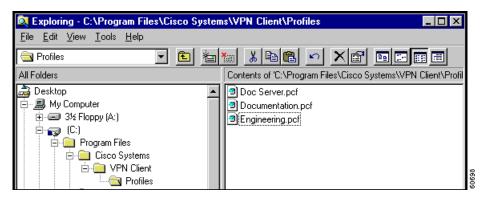
The VPN Client uses parameters that must be uniquely configured for each remote user of the private network. Together these parameters make up a user profile, which is contained in a profile configuration file (.pcf file) in the VPN Client user's local file system in the following directories:

- For Windows platforms—Program Files\Cisco Systems\VPN Client\Profiles (if the software installed in the default location)
- For the Linux, Solaris, and Mac OS X platforms—/etc/CiscoSystemsVPNClient/Profiles/

These parameters include the authentication type used, remote server address, IPsec group name and password, use of a log file, use of backup servers, and automatic Internet connection via Dial-Up Networking among many other features and requirements. Each connection entry has its own .pcf file. For example, if you have three connection entries, named Doc Server, Documentation, and Engineering, the Profiles directory shows the list of .pcf files.

Figure 5-2 shows the directory structure for the user profile in the Windows platforms.

Figure 5-2 List of .pcf files



Features Controlled by Connection Profiles

A connection profile (.pcf file) controls the following features on all platforms):

- Description of the connection profile
- The remote server address
- Authentication type
- Name of IPsec group containing the remote user
- · Group password
- · Connecting to the Internet via dial-up networking
- · Name of remote user
- · Remote user's password
- · Backup servers
- Split DNS
- Type of dial-up networking connection

- · Transparent tunneling
- TCP tunneling port
- Allowing of local LAN access
- Enabling of IKE and ESP keepalives
- Setting of peer response time-out
- · Certificate parameters for a certificate connection
- · Setting of certificate chain
- · Diffie-Hellman group
- · Verification of the DN of a peer certificate
- RADIUS SDI extended authentication setting
- · Use of SDI hardware token setting
- Split DNS setting
- Use legacy IKE port setting

A connection profile (.pcf file) controls the following additional features on the Windows platform:

- Dial-Up networking phone book entry for Microsoft
- Command string for connecting through an ISP
- · NT domain
- · Logging on to Microsoft Network and credentials
- Change the default IKE port from 500/4500 (must be explicitly added)
- Enable Force Network Login, which forces a user on Windows NT, Windows 2000, and Windows XP to log out and then log back in to the network without using cached credentials
- Enable/disable the browser proxy setting on the VPN Client for all connection types

Sample .pcf file



Connection profiles for the VPN Client are interchangeable between platforms. Keywords that are specific to the Windows platform are ignored by other platforms.

The sample .pcf profile that follows is a connection entry that uses pre-shared keys. Note that the enc_prefix (for example, enc_GroupPwd) indicates that the value for that parameter is encrypted and will be filled in by the VPN Client.

[main]

Description=connection to TechPubs server

Host=10.10.99.30

AuthType=1

GroupName=docusers

GroupPwd=

enc_GroupPwd=158E47893BDCD398BF863675204775622C494B39523E5CB65434D3C851ECF2DCC8BD488857EFAFDE1397A95E01910CABECCE4E040B7A77BF

EnableISPConnect=0

ISPConnectType=0

ISPConnect=

ISPCommand=

Username=alice

SaveUserPassword=0

```
UserPassword=
enc_UserPassword=
NTDomain=
EnableBackup=1
BackupServer=Engineering1, Engineering2, Engineering 3, Engineering4
EnableMSLogon=0
MSLogonType=0
EnableNat=1
EnableLocalLAN=0
TunnelingMode=0
TCPTunnelingPort=10000
CertStore=0
CertName=
CertPath=
CertSubjectName
SendCertChain=0
VerifyCertDN=CN="ID Cert",OU*"Cisco",ISSUER-CN!="Entrust",ISSUEE-OU!*"wonderland"
DHGroup=2
PeerTimeOut=90
ForceNetLogin=1
```

You can configure the VPN Client for remote users by creating a profile configuration file for each connection entry and distribute the .pcf files with the VPN Client software. These configuration files can include all, or only some, of the parameter settings. Users must configure those settings not already configured.

You can also distribute the VPN Client to users without a configuration file and let them configure it on their own. In this case, when they complete their configuration using the VPN Client program, they are in effect creating a .pcf file for each connection entry, which they can edit and share.

To protect system security you should *not* include key security parameters such as the IPsec group password, authentication username, or authentication password in .pcf files for remote users.



Whatever preconfiguring you provide, you must supply users with the information they need to configure the VPN Client. See "Gathering Information You Need" in Chapter 2 of the VPN Client User Guide for your platform.

Creating a .pcf file for a Connection Profile

Each user requires a unique configuration file. Use Notepad or another ASCII text editor to create and edit each file. Save as a text-only file with no formatting.

Naming the Connection Profile

For a Windows platform, you can create profile names that contain spaces. However, if you want to distribute profiles to other platforms (Linux, Mac OS X, or Solaris), the name cannot contain spaces.

Connection Profile Configuration Parameters

Table 5-2 lists all parameters, keywords, and values. It also includes the VPN Client parameter name (if it exists) that corresponds to the keyword and where it is configured on the VPN Client GUI.

You can configure each parameter on all VPN Client platforms unless specified.

Table 5-2 .pcf file parameters

.pcf Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client Configuration Location(s)
[main]	(No VPN Client field) Required keyword to identify main section.	[main] As the first entry in the file, enter exactly as shown.	Does not appear in GUI
Description=	Description A line of text that describes this connection entry. Optional.	Any text. Maximum 246 alphanumeric characters.	Connection Entry> New/Modify
Host=	Remote server address The hostname or IP address of the Cisco remote access server (a VPN central-site device) to which remote users connect.	Internet hostname, or IP address in dotted decimal notation. Maximum 255 alphanumeric characters.	Connection Entry > New/Modify
AuthType=	Authentication type For a description of authentication and authentication types, see the VPN Client user guides for the platform you are using.	The authentication type of this user: 1 = Pre-shared keys (default) 3 = Digital Certificate using an RSA signature. 5 = Mutual authentication (see note below)	Connection Entry > New/Modify > Authentication

Note Setting up mutual or hybrid authentication for users:

To use this authentication method, the VPN central-site device must have an identity certificate installed derived from a root certificate that matches the root certificate installed on the VPN Client system (the credentials used by both sides must match for mutual trust to take place). For information on how to provide a root certificate to a remote user during installation, consult the installation section in the user guide for the platform you are using. For VPN Concentrator configuration information see Configuring Mutual Group Authentication, page 1-13.

	2		1 0
GroupName=	Group Name The name of the IPsec group that contains this user. Used with pre-shared keys.	The exact name of the IPsec group configured on the VPN central-site device. Maximum 32 alphanumeric characters. Case-sensitive.	Connection Entry > New/Modify > Authentication
GroupPwd=	Group Password The password for the IPsec group that contains this user. Used with pre-shared keys. The first time the VPN Client reads this password, it replaces it with an encypted one (enc_GroupPwd).	The exact password for the IPsec group configured on the VPN central-site device. Minimum of 4, maximum 32 alphanumeric characters. Case-sensitive clear text.	Connection Entry > New/Modify > Authentication
encGroupPwd=	The password for the IPsec group that contains the user. Used with pre-shared keys. This is the scrambled version of the GroupPwd.	Binary data represented as alphanumeric text.	Does not appear in GUI.

Table 5-2 .pcf file parameters (continued)

.pcf Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client Configuration Location(s)
EnableISPConnect= (Windows-only)	Connect to the Internet via Dial-Up Networking	0 = Disable (default) 1 = Enable	Connection Entry > New/Modify > Dial-Up >
	Specifies whether the VPN Client automatically connects to an ISP before initiating the IPsec connection; determines whether to use PppType parameter.	The VPN Client GUI ignores a read-only setting on this parameter.	Connect to the Internet via dial-up
<pre>ISPConnectType= (Windows-only)</pre>	Dial-Up Networking connection entry type	0 = ISPConnect (default) 1 = ISPCommand	Connection Entry > New/Modify > Dial-Up >
	Identifies the type to use: ISPConnect or ISPCommand.	The VPN Client GUI ignores a read-only setting on this parameter.	(choosing either DUN or Third Party (command)
ISPConnect= (Windows-only)	Dial-Up Networking Phonebook Entry (Microsoft)	phonebook_name This variable is the name of	Connection Entry > New/Modify > Dial-Up >
	Use this parameter to dial into the Microsoft network; dials the specified dial-up networking phone book entry for the user's connection. Applies only if EnableISPconnect=1	the phone book entry for DUN – maximum of 256 alphanumeric characters. The VPN Client GUI ignores a read-only setting on this	Microsoft Dial-Up Networking > Phonebook
ISPCommand=	and ISPConnectType=0. Dial-Up Networking Phonebook	parameter. command string	Connection Entry >
(Windows-only)	Entry (command) Use this parameter to specify a command to dial the user's ISP dialer. Applies only if EnableISPconnect=1 and ISPConnectType=1.	This variable includes the pathname to the command and the name of the command complete with arguments; for example: c:\isp\ispdialer.exe dialEngineering Maximum 512 alphanumeric characters.	New/Modify >Dial-Up > Third party dialup program > Application
Username=	User Authentication: Username The name that authenticates a user as a valid member of the IPsec group	The exact username. Case-sensitive, clear text, maximum of 32 characters.	Connection Entry > New/Modify > Authentication
	specified in GroupName.	The VPN Client prompts the user for this value during user authentication.	

Table 5-2 .pcf file parameters (continued)

.pcf Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client Configuration Location(s)
UserPassword=	User Authentication: Password The password used during extended authentication.	Maximum of 32 alphanumeric characters, case sensitive.	Connection Entry > New/Modify > Authentication
	The first time the VPN Client reads this password, it saves it in the file as the enc_UserPassword and deletes the clear-text version. If SaveUserPassword is disabled, then the VPN Client deletes the UserPassword and does not create an encrypted version.		
	You should only modify this parameter manually if there is no GUI interface to manage profiles.		
encUserPassword	Scrambled version of the user's password	Binary data represented as alphanumeric text.	Does not appear in GUI.
SaveUserPassword	Determines whether or not the user password or its encrypted version are valid in the profile.	0 = (default) do not allow user to save password information locally.	Does not appear in GUI.
	This value is pushed down from the VPN central-site device.	1 = allow user to save password locally.	
NTDomain= (Windows-only)	User Authentication: Domain The NT Domain name configured for the user's IPsec group. Applies only to user authentication via a Windows NT Domain server.	NT Domain name. Maximum 14 alphanumeric characters. Underbars are not allowed.	Connection Entry > New/Modify
EnableBackup=	Enable backup server(s) Specifies whether to use backup servers if the primary server is not available.	0 = Disable (default) 1 = Enable	Connection Entry > New/Modify > Backup Servers
BackupServer=	(Backup server list)	Legitimate Internet	Connection Entry >
	List of hostnames or IP addresses of backup servers.	hostnames, or IP addresses in dotted decimal notation.	New/Modify > Backup Servers
	Applies only if EnableBackup=1.	Separate multiple entries by commas. Maximum of 255 characters in length.	
EnableMSLogon=	Logon to Microsoft Network.	0 = Disable	Connection Entry >
(Windows-only)	Specifies that users log on to a Microsoft network.	1 = Enable (Default)	New/Modify > Microsoft Logon
	Applies only to systems running Windows 9x.		This is available only on Windows 98 and Windows ME.

Table 5-2 .pcf file parameters (continued)

.pcf Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client Configuration Location(s)
MSLogonType= (Windows-only)	Use default system logon credentials.	0 = (default) Use default system logon credentials;	Connection Entry > New/Modify > Microsoft
	Prompt for network logon credentials.	i.e., use the Windows logon username and password. 1 = Prompt for network	Logon This is available only on
	Specifies whether the Microsoft network accepts the user's Windows username and password for logon, or whether the Microsoft network prompts for a username and password.	logon username and password.	Windows 98 and Windows ME.
	Applies only if EnableMSLogon=1.		
EnableNat=	Enable Transparent Tunneling.	0 = Disable	Connection Entry >
	Allows secure transmission between the VPN Client and a secure gateway through a router serving as a firewall, which may also be performing NAT or PAT.	1 = Enable (default)	New/Modify > Transport
TunnelingMode=	Specifies the mode of transparent tunneling, over UDP or over TCP; must match that used by the secure gateway with which you are connecting.	0 = UDP (default) 1 = TCP	Connection Entry > New/Modify > Transport
TCPTunnelingPort=	Specifies the TCP port number, which must match the port number configured on the secure gateway.	Port number from 1 through 65545 Default = 10000	Connection Entry> New/Modify > Transport
EnableLocalLAN=	Allow Local LAN Access.	0 = Disable (default)	Connection Entry >
	Specifies whether to enable access to resources on a local LAN at the Client site while connected through a secure gateway to a VPN device at a central site.	1 = Enable	New/Modify > Transport
PeerTimeout=	Peer response time-out	Number of seconds	Connection Entry >
	The number of seconds to wait before terminating a connection because the VPN central-site device on the other end of the tunnel is not responding.	Minimum = 30 seconds Maximum = 480 seconds Default = 90 seconds	New/Modify > Transport

Table 5-2 .pcf file parameters (continued)

.pcf Paran (Keyword)		VPN Client Parameter Description	Values	VPN Client Configuration Location(s)
CertStore	<u>;</u> =	Certificate Store	0 = No certificate (default)	Windows GUI
		Identifies the type of store containing the configured certificate.	1 = Cisco 2 = Microsoft The VPN Client GUI ignores	Does not appear in GUI. You can view on Certificates tab.
			a read-only (!) setting on this	Mac OS X GUI
			parameter. (See note)	Connection Entry > New/Modify > Transport
the	e value of the	arameter is marked as read only, the G parameter. However, this is not true for s can change them in the GUI display,	or Certificate parameters. These	e values cannot be overwritter
CertName=	=	Certificate Name Identifies the certificate used to	Maximum 129 alphanumeric characters	Certificates > View
	Identifies the certificate used to connect to a VPN central-site device.	The VPN Client GUI ignores a read-only setting on this parameter.		
CertPath=	The complete pathname of the directory containing the certificate file.	Maximum 259 alphanumeric characters	Certificates > Import	
		The VPN Client GUI ignores a read-only setting on this parameter.		
name (DN) of present, the V	ectName	The fully qualified distinguished name (DN) of certificate's owner. If	Either do not include this parameter or leave it blank.	Certificates > View
	present, the VPN Dialer enters the value for this parameter.	The VPN Client GUI ignores a read-only setting on this parameter.		
CertSeria	alHash	A hash of the certificate's complete contents, which provides a means of	Either do not include this parameter or leave it blank.	Certificates > View
validating the authenticity of the certificate. If present, the VPN Dialer enters the value for this parameter.		The VPN Client GUI ignores a read-only setting on this parameter.		
Ce Ce	ertSerialHash ertSubjName ertName	g certificate authentication, the softwa certificates with the same DN or CN,		
SendCert(Sends the chain of CA certificates	0 = disable (default)	Connection Entry >
		between the root certificate and the identity certificate plus the identity	1 = enable	New/Modify • Certificates > Export
		certificate to the peer for validation		•

of the identity certificate.

Table 5-2 .pcf file parameters (continued)

.pcf Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client Configuration Location(s)
VerifyCertDN	Prevents a user from connecting to a valid gateway by using a stolen but valid certificate and a hijacked IP address. If the attempt to verify the domain name of the peer certificate fails, the client connection also fails.	Include any certificate DN values of both subject and issuer: You can use all valid ASCII characters including@<>()., as well as wildcards. See example:	Does not appear in GUI

Example: VerifyCertDN=CN="ID Cert",OU*"Cisco",ISSUER-CN!="Entrust",ISSUER-OU!*"wonderland" CN="ID Cert"—Specifies an exact match on the CN.

OU*"Cisco"—Specifies any OU that contains the string "Cisco".

ISSUER-CN!"Entrust"—Specifies that the Issuer CN must not equal "Entrust".

ISSUER-OU!*"wonderland"—Specifies that the Issuer OU must not contain "wonderland".

DHGroup	Allows a network administrator to override the default group value on a VPN device used to generate Diffie-Hellman key pairs.	1 = modp group 1 2 = modp group 2 (default) 5 = modp group 5 Note: This value is preset only for pre-shared keys; for a certificate-authenticated connection, the DHGroup number is negotiated.	Does not appear in GUI
RadiusSDI	Tells the VPN Client to assume that Radius SDI is being used for extended authentication (XAuth).	0 = No (default) 1 = Yes	If this parameter is enabled, the prompts in the GUI for SDI authentication are from Radius SDI and configured using parameters in the vpnclient.ini file.
SDIUseHardwareToken	Enables a connection entry to avoid using RSA SoftID software.	0 = Yes, use RSA SoftID (default) 1 = No, ignore RSA SoftID software installed on the PC.	Does not appear in GUI
EnableSplitDNS	Determines whether the connection entry is using splitDNS, which can direct packets in clear text over the Internet to domains served through an external DNS or through an IPsec tunnel to domains served by a corporate DNS. This feature is configured on the VPN 3000 Concentrator and is used in a split-tunneling connection. Note You must also enable this feature on the VPN central-site device you are connecting to.	0 = No 1 = Yes (default)	Does not appear in GUI

Table 5-2 .pcf file parameters (continued)

.pcf Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client Configuration Location(s)
UseLegacyIKEPort	Changes the default IKE port from 500/4500 to dynamic ports to be used during all connections. You must explicitly enter this parameter into the .pcf file.	0 = (default with Release 4.8.01 and higher) Turn off the legacy setting; use dynamic ports with cTCP. 1 = Maintain the legacy setting 500/4500. This lets TCP/UDP work easily with VPN central-site devices that support cTCP. This setting enables interoperability with VPN central-site devices that expect the VPN Client to use static port assignments. Enabling this parameter inhibits interoperability with certain versions of Windows.	Does not appear in GUI
ForceNetlogin (windows-only)	Enables the Force Net Login feature for this connection profile.	0 = Do not force the user to log out and log in (default). 1 = Force user to log out when the Wait time is reached unless an option is selected. 2 = Disconnect VPN session upon reaching the Wait time unless an option is selected. 3 = Wait for the user to select Connect or Disconnect.	Does not appear in GUI
ForceNatT	Causes the VPN Client to negotiate NAT-T when available, even if there is no NAT device involved in the connection attempt. This helps with some firewalls' disconnecting the VPN Client unexpectedly.	ForceNatT=0 (default) ForceNatT=1 (Negotiate NAT-T when available)	Does not appear in GUI.
In the following rows between connections	s, the use of the "!" character in the profil	e prevents the previous user's in	nformation from being retained
CertMatchDN	Allows wildcard matches of Distinguished Name certificate fields for certificate selection by the VPN Client.	CertMatchDN=CN="ID Cert", OU* "Cisco", Issuer-CN!= "Entrust", Issuer-OU!*"wonderland"	Does not appear in GUI.

Table 5-2 .pcf file parameters (continued)

.pcf Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client Configuration Location(s)
CertMatchKU	Allows wildcard matches of Key Usage certificate fields for certificate selection by the VPN Client.	CertMatchKU=0,3,4,5	Does not appear in GUI.
CertMatchEKU	Allows wildcard matches of Extended Key Usage certificate fields for certificate selection by the VPN Client. This keyword applies to connection attempts only and not to any other certificate-related operation (such as listing certificates, viewing certificates, and so on). This keyword applies to all forms of certificate selection (such as CertSerialHash, CertMatchDN, CertSubjectName, or CertName). The value of this keyword is a comma-separated list of Extended Key Usage OID strings. Custom Extended Key Usage strings must be of the form 1.3.6.1.5.5.7.3.n, where n can be any number.	CertMatchEKU=1.3.6.1.5.5. 7.3.2,1.3.6.1.5.5.7.3.1 where: 1.3.6.1.5.5.7.3.2 = Client authentication 1.3.6.1.5.5.7.3.1 = Server Authentication	Does not appear in GUI.

Distributing Configured VPN Client Software to Remote Users

When you have created the VPN Client profile configuration file, you can distribute it to users separately or as part of the VPN Client software.

Separate Distribution

To distribute the configuration file separately and have users import it to the VPN Client after they have installed it on their PCs, follow these steps:



For the Mac OS X platform, the configuration file is placed in the Profiles folder before the VPN Client is installed. See Chapter 2 of the VPN Client User Guide for Mac OS X for more information.

- Step 1 Distribute the appropriate profile files to users on whatever media you prefer.
- Step 2 Supply users with necessary configuration information.
- Step 3 Instruct users to:
 - a. Install the VPN Client according to the instructions in the VPN Client User Guide for your platform.
 - b. Start the VPN Client and follow the instructions in Chapter 5 of the *VPN Client User Guide* for your platform. See the section "Importing a VPN Client Configuration File." (Windows-only)

- c. Finish configuring the VPN Client according to the instructions in Chapter 4of the VPN Client User Guide for your platform.
- **d**. Connect to the private network, and enter parameters according to the instructions in Chapter 5 of the *VPN Client User Guide* for your platform.

Distribution with the VPN Client Software

If the vpnclient.ini file is bundled with the VPN Client software when it is first installed, it automatically configures the VPN Client during installation. You can also distribute the profile files (one .pcf file for each connection entry) as preconfigured connection profiles for automatic configuration.

To distribute preconfigured copies of the VPN Client software to users for installation, perform the following steps:

Step 1 Copy the VPN Client software files from the distribution CD-ROM into each directory where you created an vpnclient.ini (global) file and separate connection profiles for a set of users.



For the Mac OS X platform, preconfigured files are placed in the Profiles and Resources folders before the VPN Client is installed. The vpnclient.ini file is placed in the installer directory. You must place custom vpnclient.ini files in the VPN Client Installer directory at the same level as the Profiles and Resources folders. See Chapter 2 of the VPN Client User Guide for Mac OS X for more information.

Step 2 Prepare and distribute the bundled software.

CD-ROM or network distribution: Be sure the vpnclient.ini file and profile files are in the same directory with all the CD-ROM image files. You can have users install from this directory through a network connection; or you can copy all files to a new CD-ROM for distribution; or you can create a self-extracting ZIP file that contains all the files from this directory, and have users download it, and then install the software.

Step 3 Supply users with any other necessary configuration information and instructions. See Chapter 2 of the *VPN Client User Guide* for your platform.



CHAPTER 6

Updating VPN Client Software on a VPN 3000 Concentrator

There are two ways to update VPN Client software. You can place a new release or update on a web server, called the *update server*, and notify remote users of all client types (Linux, Windows, Mac OS X and so on) where to retrieve and install the updated software. Or, starting with Release 4.6, you can automatically update VPN Client software for Windows 2000 and Windows XP remote users.

This section has the following sections:

Enabling Client Update (All Client Types)

Updating the VPN Client Software Automatically on Windows 2000 and Windows XP Systems

Managing Autoupdates

How Automatic Update Works

For additional information, see the autoupdate white paper in the same download location as the VPN Client Update files on www.cisco.com.

Enabling Client Update (All Client Types)

To update VPN Client software, you must enable Client Update on the VPN Concentrator. When you enable Client Update, you notify VPN Client users that it is time to update the VPN Client software on their remote systems. The notification includes a location containing the update package (the update does not happen automatically).



Each update folder on the web server must contain only one version package from Cisco. If you need more than one version, configure more groups on the VPN Concentrator to update from different web server folders.

Use the Client Update procedure at the VPN 3000 Concentrator to configure a client notification:

- Step 1 To enable Client Update, go to Configuration | System | Client Update and click **Enable**.
- Step 2 At the Configuration | System | Client Update | Enable screen, check **Enabled** (the default) and then click **Apply**.
- Step 3 On the Configuration | System | Client Update | screen, click Entries.

- Step 4 On the Entries screen, click **Add**. The VPN Concentrator Manager, displays the Configuration | System | Client Update | Entries | Add or Modify screen.
- **Step 5** For Client Type, enter the operating systems to notify:
 - Windows includes all Windows based platforms.
 - Win9X includes Windows 95, Windows 98, and Windows ME platforms.
 - WinNT includes Windows NT 4.0, Windows 2000, Windows XP, and Windows Vista platforms.
 - · Linux.
 - Solaris.
 - Mac OS X.



Note

The VPN 3000 Concentrator sends a separate notification message for each entry in a Client Update list. Therefore your client update entries must not overlap. For example, the value Windows includes all Windows platforms, and the value WinNT includes Windows NT 4.0, Windows 2000 and Windows XP platforms. So you would not include both Windows and WinNT. To find out the client types and version information, click on the lock icon at the top left corner of the Cisco Systems VPN Client main window and choose **About VPN Client**.

Step 6 In the URL field, enter the URL that contains the notification.

To activate the Launch button on the VPN Client Notification, the message must include the protocol HTTP or HTTPS and the server address of the site that contains the update. The message can also include the directory and filename of the update, for example, http://www.oz.org/upgrades/clientupdate. If you do not want to activate the Launch button for the remote user, you do not need to include a protocol in the message.

- Step 7 In the Revisions field, enter a comma separated list of client revisions that do not need the update because they are already using the latest software. For example, the value 4.0 (Rel), 4.0.3 identifies the releases that are compliant; all other VPN Clients need to upgrade.
- Step 8 Click Add.

The Notification dialog box appears when the remote user first connects to the VPN device or when the user clicks the Notifications button on the Connection Status dialog box. When the notification pops up, on the VPN Client, click **Launch** on the Notification dialog box to open a default browser and access the URL containing the update.

Updating the VPN Client Software Automatically on Windows 2000 and Windows XP Systems

The VPN Client for Windows 2000 and Windows XP software can securely download updates and new versions automatically through a tunnel from a VPN 3000 Concentrator or other VPN server that can provide notifications.

With this feature, called *autoupdate*, users do not need to uninstall an old version of the software, reboot, install the new version, and then reboot again. Instead, an administrator makes updates and profiles available on a web server and when a remote user starts up the VPN Client, the software detects that a download is available and automatically gets it.

If a new version requires reboots (during a major upgrade), the remote user has to reboot only twice, when the program uninstalls the old version and when download completes. If the new version does not require a reboot, as in a minor update, autoupdate notifies users that they do not need to reboot. Also, if a user interrupts the download by disconnecting the VPN Client and then later reconnects, the download resumes at the point where it was interrupted.

Managing Autoupdates

This section explains the manager tasks needed to automatically update VPN Client software. Generally, an administrator is responsible for performing the following tasks:

- Setting up a web server to contain the download packages, called the *update server*. The packages contain update-x.x.xx.xxxx-minor/major-K9 files, provided by Cisco Systems. This procedure outline assumes that you already know how to set up web servers and does not include instructions for doing so.
- Enabling the VPN Concentrator to perform autoupdates.
- Obtaining the latest version package from Cisco.
- Creating the profile bundle—a package containing new or revised profiles (.pcf files) (optional).
- Changing the version information file (new_update_config.ini) (optional).
- Creating oem zip packages and enter the names of these packages into the new_update_config.ini file (optional).



VPN Client automatic updating does not support Windows Vista.

Prerequisite

Remote users must have the VPN Client for Windows 4.6 or greater installed on their PCs to use the automatic update feature.

Enabling Client Update for Automatic Updates

The procedure for configuring Client Update on the VPN Concentrator for automatic updating VPN Client software is a subset of the notification feature described in the section "Enabling Client Update (All Client Types)." For detailed information about how to configure Client Update, you should read the Client Update section of *Cisco VPN 3000 Series Concentrator Reference, Vol. I: Configuration*.

For information about how to configure Client Update on a Cisco ASA Series 5500 Adaptive Security Appliance using ASDM, see Configuring Client Software Update Using ASDM, page 2-13. To use the command-line interface to do this, see Configuring Client Software Update Using ASDM, page 3-9.

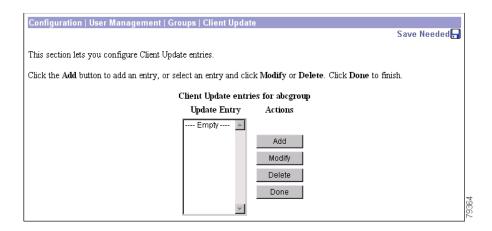
To enable Client Update on the VPN 3000 Sesries Concentrator, use the procedure in the section "Enabling Client Update (All Client Types)."

You may want to create a group especially for autoupdate; use the following procedure.

Step 1 To enable Client Update at the VPN group level, go to Configuration | User Management | Groups.

- Step 2 To add a new group especially for automatic updates, click **Add** and enter the name of the group. Then click **Apply**. The new group appears in the Current list. Now you can select the group and modify it for Client Update.
- Step 3 Next too modify a group in the Current list for Client Update, select the group and click **Client Update**. The manager displays the Client Update screen.

Figure 6-1 VPN Concentrator Client Update Screen



- Step 4 When you get to the Client Update | Entries | Add or Modify screen, enter information into the fields as follows:
 - a. Enter the Client Type information. Since autoupdate runs only on Windows 2000 and Windows XP, all other client types update manually. So for example, enter WinNT. This choice automatically updates Windows 2000 and Windows XP users, while Windows NT users get notified and can get an update manually from the update server.
 - **b.** In the URL field, enter the URL of the update server that contains the update download package and the notification. The URL must contain **http://**; for example, http://update_server_engineering.
 - c. Enter the revision for this autoupdate; for example, update-4.6.
- Step 5 Click Add or Apply.

When the VPN Client software gets the notification, it launches the autoupdate program and gives it the location from which to download the updated version and profiles (if there are any).

Getting the Updated Software from Cisco Systems

The installation package that the VPN Client software downloads from the update server can be either a completely new release (a full install) or an update. A new (major) release has a name in the form update-x.x.xx.xxxx-major-K9.zip and a minor release has a name in the form update-x.x.xx.xxxx-minor-K9.zip. You can download the latest VPN Client software from the following location:

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

Each full release of the VPN Client for Windows software requires the following objects:

- vpnclient-win-msi-x.x.int_x-k9.exe—the Microsoft installation file; for example, vpnclient-win-msi-5.0.04.0300-k9.exe or vpnclient-win-msi-5.0.4rel-k9.exe—VPN Client Software for 2000/XP/Vista Microsoft Installer, or vpnclient-win-msi-5.0.04.0300-k9-jp_wohelp.exe—Japanese VPN Client Software for 2000/XP/Vista without online help Microsoft Installer.
- update-5.0.04.0300-major-K9.zip—Windows AutoUpdate Component Zip File.
- ReadMe File for 5.0.04.0300.
- sig.dat—a signature file containing a signature of binary.zip and the MSI installation file. This file
 is used for the verification process to ensure that these files have not been tampered with. When
 autoupdate finishes downloading the update, it deletes this file.
- binary_config.ini—a configuration file listing the version available on the update server. Autoupdate uses this file to determine whether it needs to go get the update. If the last major version number (for example, 5.0.4.0300) in this file is greater than the current version, autoupdate downloads a full install. If not, then autoupdate looks at the version field. If the version number is greater than the current version (for example, 4.6.1.1) on the PC, autoupdate downloads an update. In any case, after autoupdate finishes downloading the update package, it deletes this file.
- new_update_config.ini—this optional configuration file is used by the autoupdate program to
 determine what custom settings to download. An administrator who is adding profiles and oem
 packages to an update must enter the names of the files that contain new or updated profiles and oem
 packages into this file. Once autoupdate has completed the update, this file becomes
 update_config.ini on the user's system.

Of these objects, an administrator is responsible only for updating the new_update_config.ini file when distributing new or updated profiles. You must not modify the other files in the package. Cisco supplies these files and they are secured by the signature in the sig.dat file.

Creating the New Update Configuration File

When distributing new or modified profiles, the administrator must enter information into the new_update_config.ini file. This file has the same structure as a standard configuration file (see "File Format for All Profile Files" section on page 5-2). Following is a sample new_update_config.ini file.

[Update] Version=1 FileName=profiles.zip MaxSize=7000

[Oem] FileName=oem.zip MaxSize=10000

[Transform]
Filename=transform.zip
MaxSize=12000

[Autoupdate] Required=1

new_update_config.ini File Keywords and Values

Table 6-1 describes each part of the new_update_config.ini file.

Table 6-1 new_update_config.ini File Parameters

Keyword	Description	Value
[Update]	Required keyword to identify update information.	Keep exactly as shown.
Version=	Version number of the update package. The administrator can use this parameter to track updates by incrementing the value each time there is a new version of this file.	Enter a value 0 or greater.
Filename=	Name of the zip file containing profiles to update or install	Enter the filename (string.zip) Example: newprofile.zip
MaxSize=	Size in bytes of the profile file plus 5000 bytes. This places a limit on how large the file can be.	Enter the size of the file plus 5000 bytes. Example: 10000
MaxSize=	Size in bytes of the oem file plus 5000 bytes. This places a limit on how large the file can be.	Enter the size of the file plus 5000 bytes. Example: 12000
[Transform]	Optional keyword to identify oem information for MSI installation.	Keep exactly as shown.
FileName=	Name of the zip file containing transform information to update or install an update to the MSI installation program.	Enter the filename (string.zip). Example: newtransform.zip
MaxSize	Size in bytes of the transform file plus 5000 bytes. This places a limit on how large the file can be.	Enter the size of the file plus 5000 bytes. Example: 14000
[Autoupdate]	Keyword to identify the autoupdate section.	Keep exactly as shown.
Required=	Indicates whether the update or profile update is required.	Enter either 0 or 1. 0 = not required 1 = required



The transform within the zip file for modifying an MSI installation must be named oem.mst.

Creating the Profile Distribution Package

To automatically distribute new or updated profiles, use the following procedure:

- Step 1 Create the new profile files or modify your current profile files. For information on how to create and modify individual profiles (.pcf files), see Creating Connection Profiles, page 5-23.
- Step 2 Create a zip file containing the updated profiles; for example, name it profiles.zip.

Step 3 Enter the name of this .zip file into the new_update_config.ini file nd increment the version number under the [Update] section of this file.



Although you do not need to update the VPN Client to update the profiles, the update server must also contain all of the required Cisco distributed update files for the VPN Client to accept the new profiles.

Step 4 Copy the new_update_config.ini and the zip file containing the new profiles onto the update server.

How Automatic Update Works

This section provides information for administrators that want to understand more about how this feature works. This is a high-level overview of the autoupdate feature.

The automatic update feature (autoupdate) comprises three processes:

- · autoupdate.exe—detects that an update package is on the update server and goes out and retrieves it
- autoinstall.exe—installs the update package
- autoupdategui.exe—handles notifications to the remote user and user responses to notifications

This is what happens:

- A remote user starts up the VPN Client and establishes a tunnel
- The VPN Client software gets the URL of the site containing the update package
- The VPN Client software starts the autoupdate.exe program and gives it the URL for the update package
- Autoupdate determines if an update is necessary by comparing the version information to the one that exists on the VPN Client PC.
- If the update package is later than the one on the PC, autoupdate downloads the update package.
- Autoupdate than lets the remote user know that the update package is available
- The remote user accepts or rejects the update package
- If the remote user accepts the update package, autoupdate verifies the integrity of the update
- Autoupdate unzips the update package then installs it
- If there are any errors, autoupdate or autoinstall logs them in the autoupdate.log and autoinstall.log files found in the Updates folder of the VPN Client folder.

How Automatic Update Works



CHAPTER

Configuring Automatic VPN Initiation—Windows Only



Before you begin, we highly recommend that you read the White Paper "Wireless LAN Security," which you can access at:

http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps430/ps4076/prod_white_paper09186a00800b469f_tk809_TSD_Technologies_White_Paper.html

This document analyzes the best practices of implementing security for wireless LANs using VPNs. For a sample configuration demonstrating complete step-by-step instructions covering the group/user configuration on a secure gateway, auto initiation configuration on the VPN Client, and wireless configuration in the Aironet, refer to the TAC technical note "Configuring Automatic VPN Initiation on a Cisco VPN Client in a Wireless LAN Environment."

Automatic VPN initiation (auto-initiation) provides secure connections within an on-site wireless LAN (WLAN) environment through a secure gateway. When auto initiation is configured on the VPN Client, the VPN Client:

- Becomes active immediately when a user starts his/her PC or when the PC becomes active after being on standby or hibernating
- Detects that the PC has an IP address defined as requiring auto initiation
- Establishes a VPN tunnel to the secure gateway defined for its network, prompts the user to authenticate, and allows that user network access

It is worth mentioning that although auto initiation was designed for wireless environments, you can use it in any networking environment. Auto initiation provides a generic way for the VPN Client to auto initiate a connection whether the VPN Client PC is based on specific networks or not.

In most cases, a saved Group and Username password best facilitates the seamless nature of this feature.



You can set up auto initiation configurations that both include and exclude networks for auto initiation.

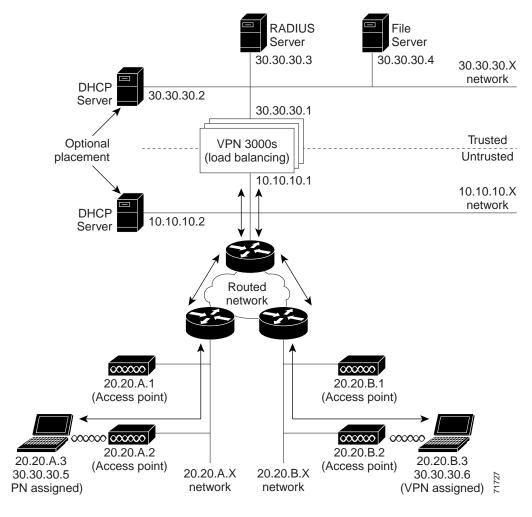
Both Linux and Mac OS X VPN Clients support auto-initiation, but they do not have a GUI component or a service to initiate the feature on bootup. The CLI command to begin auto-initiation on these non-Windows Clients is **vpnclient autoinit**.



Auto-initiation on Windows does not replace the Start Before Logon feature. Auto-initiation activates after the user has logged on.

Figure 7-1 depicts a simple network configuration that employs VPN for securing on-site WLANs. The secure gateways, in this case VPN 3000 Concentrators, which may or may not be using load balancing, provide the gateway between the untrusted and the trusted networks. The DHCP Server can be on either side of the VPN 3000 Concentrator. VPN Client users with laptops that have wireless NIC cards can connect through access points (APs) throughout the campus or building and tunnel to the trusted 30.30.30.x network from the untrusted 10.10.10.x network. The network administrator can set this type of scenario up to be largely transparent to the VPN Client user.

Figure 7-1 Auto Initiation Scenario



In Figure 7-1 the trusted (wired) network, numbered 30.30.30, is at the top of the diagram with a VPN Concentrator separating it from other networks considered untrusted. The untrusted networks contain wireless subnets, such as 20.20.A.x and 20.20.B.x. Every device on the untrusted network must use a VPN tunnel to access resources on the trusted network. Access to a DHCP server must be available to provide the devices on the untrusted network with initial IP connectivity to the VPN Concentrator. The figure shows the placement of the DHCP server as optional, since it can be placed either on the untrusted network or on the trusted network with DHCP Relay enabled in the VPN Concentrator.

To configure auto initiation for users on the network, you add parameters to the VPN Client's global profile (vpnclient.ini). For information on how to create or use a global profile, see Creating a Global Profile, page 5-2.

Using the VPN Client GUI, users can only enable/disable auto initiation and change the retry interval. These features are available through the Options menu when auto initiation has been configured through the global profile. If auto initiation is not configured, these options do not appear in the Options menu. For a complete explanation of how auto initiation appears to the VPN Client user on a Windows system, see *Cisco VPN Client User Guide for Windows*, "Using Automatic VPN Initiation."

The auto initiation feature can be used in WLAN environments containing NIC cards and access points from any vendor.

Creating Automatic VPN Initiation in the vpnclient.ini File

This section shows how to create or edit the vpnclient.ini file to activate auto initiation on a VPN Client.

Preparation

Before you begin, you should gather the information you need to configure auto initiation:

- The network IP addresses for the client network
- · The subnet mask for the client network
- The names for all connection entries that users are using for their connections

What You Have to Do

To configure auto initiation, you must add the following keywords and values in the [Main] section of the vpnclient.ini global profile file:

- AutoInitiationEnable—enables or disables auto initiation. To enable auto initiation, enter 1. To
 disable it, enter 0.
- AutoInitiationRetryInterval—specifies the number of minutes to wait before retrying an auto
 initiation connection. The range is 1 to 10 minutes or 5 to 600 seconds. If you do not include this
 parameter in the file, the default retry interval is one minute.
- AutoInitiationRetryIntervalType—specifies whether the retry AutoInitiationRetryInterval
 parameter is displayed in minutes or seconds. The default is 0 (meaning minutes). Set this parameter
 to 1 to indicate seconds.
- AutoInitiationList—provides a series of section names, each of which contains a network address, a subnet mask, a connection entry name, and optionally, a connect flag. You can include a maximum of 64 section (network) entries.
 - The section name is the name of an entry in the auto initiation list (within brackets)
 - The network and subnet mask identify a subnet
 - The connection entry specifies a connection profile (.pcf file) configured for auto initiation.
 - The connect flag, if present, indicates the action to take if there is a match. If the Connect parameter is set to 1, the VPN Client should auto initiate; if 0, the VPN Client should not auto initiate. The default setting is 1. This parameter is optional. You can use it to exclude certain network ranges from auto initiation. For example, you might want to address a situation where Mobile IP and VPN software clients co-exist on client PCs and you want the VPN Client to auto initiate when not on a corporate subnet.

In general, when configuring exceptions with the Connect parameter, you might want to place the network ranges you are excluding before those that should auto initiate. More importantly, the software processes the list in the order specified in the vpnclient.ini file. When it matches an entry in the list, the software stops searching and the Connect setting of that entry determines whether to auto initiate or do nothing. So if you put the Connect = 1 entries first, the software never reaches the Connect=0 entries.

It is also important to order the entries in the list by the uniqueness of the network and subnet mask. You should list the more unique entries first. For example, an entry with a network/mask that specifies a match on 10.10.200.* should come before a network/mask that specifies a match on 10.10.*.* If not, the software matches 10.10.*.* and never reaches 10.10.200.*

Here is an example of an entry in an auto initiation list that excludes the network from auto initiating:

[Franklin] Network=10.10.200.0 Subnet=255.255.255.0 ConnectionEntry=robron Connect=0

Example 7-1 Section of vpnclient.ini File for Auto Initiation

Suppose a sales manager travels among three locations (Chicago, Denver, and Laramie) within a corporation, attending sales meetings, and wants to securely and easily initiate a wireless connection at these locations. The vpnclient.ini contains the entries shown in this example. The connection entry named in each network section points to the individual's profile (.pcf) for that on-site wireless LAN network.

```
[Main]
AutoInitiationEnable=1
AutoInitiationRetryInterval=3
AutoInitiationList=ChicagoWLAN, DenverWLAN, LaramieWLAN
[ChicagoWLAN]
Network=110.110.110.0
Mask=255.255.255.0
ConnectionEntry=Chicago (points to a connection profile named chicago.pcf)
[DenverWLAN]
Network=220.220.220.0
Mask=255.255.255.0
ConnectionEntry=Denver (points to a connection profile named denver.pcf)
[LaramieWLAN]
Network=221.221.221.0
Mask=255.255.255.0
ConnectionEntry=Laramie (points to a connection profile named laramie.pcf)
```

Example 7-2 Section of vpnclient File for Auto Initiation that excludes and includes auto initiation

In this example, the exceptions (more specific) network addresses appear first in the vpnclient.ini file followed by the connection entries for auto initiation. The connection entries for auto initiation do not need to include the Connect parameter.

```
[Main]
AutoInitiationEnable=1
AutoInitiationRetryInterval=3
AutoInitiationList=NetworkAExceptions, NetworkA, NetworkBexceptions, NetworkB
[NetworkAExceptions]
Network=192.168.0.0
Mask=255.255.255.0
ConnectionEntry=VPNprofileA1
Connect=0
```

[NetworkA]
Network=192.0.0.0
Mask=255.0.0.0
ConnectionEntry=VPNprofileA2
[NetworkBExceptions]
Network=161.200.100.0
Mask=255.255.255.0
ConnectionEntry=VPNprofileB1
Connect=0
[NetworkB]
Network=161.200.0.0
Mask=255.255.0.0
ConnectionEntry=VPNprofileB2

Example 7-3 Section of vpnclient File for Auto-initiation That Always Uses Auto-initiation

In the following example, the VPN Client is configured to always attempt to establish a connection independent of the network address discovered.

[Main]
AutoInitiationEnable=1
AutoInitiationRetryInterval=3
AutoInitiationList=NetworkAll
[NetworkAll]
Network=0.0.0.0
Mask=0.0.0.0
ConnectionEntry=VPNprofileName
Connect=1

Verifying Automatic VPN Initiation Configuration

To verify that you have configured auto initiation correctly, open the VPN Client GUI application and perform the following steps:

- Step 1 Display the Options menu, and select **Automatic VPN Initiation**.
- Step 2 On the Automatic VPN Initiation dialog, verify that Enable automatic VPN initiation is selected. If not, then click to select it.
- Step 3 Click Apply to close the window.

Alternatively you can verify the auto initiation configuration from the command line by executing the following command:

vpnclient verify autoinitconfig

This display shows configuration information for each setting plus a list of your network entries.

C:\Program Files\Cisco Systems\cd UPN Client

C:\Program Files\Cisco Systems\UPN Client\vpnclient verify autoinitconfig Cisco Systems UPN Client Uersion 4.0 (int_92)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.0.2195

Auto-initiation Configuration Information.
Enable: 1
Retry Interval: 2 minutes
List Entry 0: Network: 10.10.32.32
Mask: 0.0.0.0
Connect Flag: 1
Connection Entry: "Engineering"



CHAPTER

Using the VPN Client Command-Line Interface

This chapter explains how to use the VPN Client command-line interface (CLI) to connect to a Cisco VPN device, generate statistical reports, and disconnect from the device. You can create your own script files that use the CLI commands to perform routine tasks, such as connect to a corporate server, run reports, and then disconnect from the server.

CLI Commands

This section lists each command, its syntax, and gives sample output for each command. It is organized by task.

Displaying a List of VPN Client Commands

To display a list of all VPN Client commands, go to the directory that contains the VPN Client software, and enter the vpnclient command at the command-line prompt:

```
C:\Program Files\Cisco Systems\UPN Client\vpnclient
Cisco Systems UPN Client Version 4.0 (int_92)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.0.2195

Usage:
    vpnclient connect \( \text{profile} \) [user \( \text{username} \)] [eraseuserpwd \; pwd \( \text{password} \)]
    vpnclient disconnect
    vpnclient stat [reset] [traffic] [tunnel] [route] [firewall] [repeat]
    vpnclient notify
    vpnclient verify [autoinitconfig]
    vpnclient resumefw
```



The **vpnclient** command lists all the commands and parameters available for your platform. Not all commands and parameters are available on all platforms.

Starting a Connection—vpnclient connect

To start a connection, enter the following command:

Table 8-1 lists the command options you can use with the vpnclient connect command, includes the task that each option performs, and gives an example of each option.

Table 8-1 Command Line Options

option	Definition	Notes and Examples
profile	Name of the connection entry (.pcf file), that you have	If the filename contains spaces, enclose it in double quotes on the command line.
	previously configured. Required.	Example: vpnclient connect "to VPN"
user	Specifies a username for authentication; with the pwd option, suppresses the username prompt in authentication dialog. Optional.	Updates the username in the .pcf file with this name. However, if the name supplied is not valid, the VPN Client displays the authentication dialog on a subsequent request.
		Example: vpnclient connect user robron pwd siltango toVPN
eraseuserpwd	Erases the user password saved on the Client PC thereby forcing the VPN Client to prompt for a password. Optional.	You might have configured a connection with Saved Password to suppress a password prompt when connecting using a batch file. You can then use the eraseuserpwd to return to the more secure state of requiring password input from the console when connecting.
		Example: vpnclient connect eraseuserpwd toVPN
pwd	Specifies a password for authentication; with the user option on the command line, suppresses the password prompt in authentication dialog. Optional.	If the password supplied is not valid, the VPN Client displays the authentication dialog on a subsequent request. After encrypting and using the password for the connection, the VPN Client clears the password in the .pcf file. Using this option on the command line compromises security and is not recommended.
		Example: vpnclient connect user robron pwd siltango toVPN
nocertpwd	Suppresses prompting for a certificate password. Optional.	Example: vpnclient connect nocertpwd toVPN
cliauth (Windows platforms only)	Prompts for authentication information on the command line. Eliminates the GUI prompt that	The VPN client prompts for username and password. The password is displayed as asterisks.
	displays during a connection request from the command line.	Example: vpnclient connect cliauth toVPN

VPN Client Administrator Guide

Table 8-1 Command Line Options

option	Definition	Notes and Examples
stdin	Causes the CLI to read input from the standard input pipe instead of from the console.	This option enables third party software to provide input directly to the CLI Example: vpnclient connect toVPN stdin
sd	Suppresses the "Do you wish to disconnect your Dial-Up Networking connection?" message that occurs when one is using Microsoft Dial-Up Networking.	Post version 4.0.3D this switch behaves as documented here. Example: vpnclient connect toVPN sd
domain	Specifies the domain for the connection.	Specify the Domain keyword last. In most cases with Radius, the Domain field is not used, so it must be NULL, as shown in the following example: vpnclient connect profile-name user name pwd password domain If the domain name is NULL, the GUI prompts the user for one.



When using the "pwd" option of the CLI, an invalid password is actually sent three times to the secure gateway. This causes problems with some authentication devices that record failed password attempts. Use the **cliauth** command, which sends the password only once and also prevents the use of a return code in scripts.

Example 8-1 vpnclient connect Command

This example shows the vpnclient connect command that connects you to the Engineering Server using the profile name "engineering"

```
C:\Program Files\Cisco Systems\UPN Client>\upnclient connect engineering Cisco Systems UPN Client Uersion 4.0 (int_92) Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved. Client Type(s): Windows, WinNT Running on: 5.0.2195
```

Initializing the UPN connection. Contacting the gateway at 10.10.32.32 Authenticating user.

87652

At this point, the VPN Client displays an authentication dialog box that prompts for your username and password.

Figure 8-1 Authenticating a User



After you enter your name and password, authentication succeeds, and the command continues executing.

Negotiating security policies. Securing communication channel. Welcome to Wonderland University You can register on line beginning March 24, 2003 Do you wish to continue? (y/n): Your UPN connection is secure.

Example 8-2 vpn connect Command Using cliauth

Alternatively, to suppress the User Authentication window shown in Example 4-1, you can use the cliauth parameter. The command line then prompts for username and password. Using the cliauth parameter avoids having a password display in clear text on the command line.

Example 8-3 vpnclient connect Command Using Parameters

The following command connects to the remote network without user interaction. Notice that the password appears on the command line in clear text.

```
C:\Program Files\Cisco Systems\UPN Client>vpnclient connect engineering user pat c pwd Mohawk3turn
Cisco Systems UPN Client Version 4.0 (int_92)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.0.2195

Initializing the UPN connection.
Contacting the gateway at 10.10.32.32
Authenticating user.
Negotiating security policies.
Securing communication channel.
Welcome to Wonderland University
You can register on line beginning March 24, 2003
Do you wish to continue? (y/n):
Your UPN connection is secure.
```

Displaying a Notification—vpnclient notify

When you connect, you can display a notification using the vpnclient notify command:

vpnclient notify

Example 8-4 vpnclient notify Command

The following session shows how to use the vpnclient notify command to display a notification from a network administrator.

```
C:\Program Files\Cisco Systems\Vpn Client\vpnclient notify
Cisco Systems VPN Client Version 4.0
Copyright <C> 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type<s>: Windows
Running on: 5.0.2195

Notification:
Your network administrator has placed an update of the Cisco Systems VPN Client at the following location:
http://www.mycompany.com/clientupdate
```

Displaying an Automatic VPN Initiation Configuration—Windows Only

To display your configuration for auto initiation, enter the following command:

vpnclient verify autoinitconfig



If the mask in the output display does not match the value in the profile, then the mask is invalid. An invalid mask is displayed as 255.255.255.255

Example 8-5 vpnclient verify Command

The following command shows your auto initiation configuration for one access point.

```
C:\Program Files\Cisco Systems\UPN Client>vpnclient verify autoinitconfig Cisco Systems UPN Client Version 4.0 (int_92)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.0.2195

Auto-initiation Configuration Information.
Enable: 0
Retry Interval: 2 minutes
List Entry 0: Network: 10.10.32.32
Mask: 0.0.0
Connect Flag: 1
Connection Entry: "Engineering"
```

Suspending/Resuming Stateful Firewall (Windows Only)

To suspend the stateful firewall, enter the following command:

```
vpnclient suspendfw
```

To resume a suspended stateful firewall, enter the following command;

```
vpnclient resumefw
```

Example 8-6 Suspending and Resuming Stateful Firewall

The following commands control the setting of the stateful firewall. The first command output shows the response displayed when the stateful firewall is not enabled when the command is executed. The next two commands, executed after enabling the stateful firewall, first suspend the firewall and then resume it.

```
C:\Program Files\Cisco Systems\UPN Client\vpnclient suspendfw
Cisco Systems UPN Client Version 4.0 (int_92)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.0.2195

The Stateful Firewall (Always On) service is disabled so it cannot be suspended or resumed

C:\Program Files\Cisco Systems\UPN Client\vpnclient suspendfw
Cisco Systems UPN Client Uersion 4.0 (int_92)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.0.2195

The Stateful Firewall (Always On) service has been suspended

C:\Program Files\Cisco Systems\UPN Client\vpnclient resumefw
Cisco Systems UPN Client Uersion 4.0 (int_92)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.0.2195

The Stateful Firewall (Always On) service has been resumed
```



If you reboot the PC after suspending the stateful firewall, the software restores the Stateful Firewall setting to enable, and this will block traffic. If the firewall is not initially enabled or suspended, the **resumefw** command does not enable the firewall.

Ending a Connection—vpnclient disconnect

To disconnect from your session, enter the following command:

vpnclient disconnect

Example 8-7 vpnclient disconnect Command

The following command disconnects you from your secure connection.

C:\Program Files\Cisco Systems\UPN Client>vpnclient disconnect Cisco Systems UPN Client Version 4.0 (int_92) Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved. Client Type(s): Windows, WinNT Running on: 5.0.2195

Disconnecting the UPN connection.
Your UPN connection has been terminated.

8

Displaying Information About Your Connection—vpnclient stat

To generate status information about your connection, enter the following command:

vpnclient stat [reset] [traffic] [tunnel] [route] [firewall] [repeat]

When entered without any of the optional parameters, the vpnclient stat command displays all status information. The following parameters are optional:

Option	Definition	Example
reset	Restarts all connection counts from zero. SA stats are not reset.	vpnclient stat reset
traffic	Displays a summary of bytes in and out, packets encrypted and decrypted, packets bypassed, and packets discarded.	vpnclient stat traffic
tunnel	Displays IPsec tunneling information.	vpnclient stat tunnel
route	Displays configured routes.	vpnclient stat routes
firewall	Identifies the type of firewall in use and displays information generated by the firewall configuration. This option is available only on Windows platforms	vpnclient stat firewall
repeat	Provides a continuous display, refreshing it every few seconds. To end the display, press <ctrl-c>.</ctrl-c>	vpnclient stat traffic repeat vpnclient stat repeat
	To first reset the statistics information, use the reset option with the repeat option (see examples).	vpnclient stat reset traffic repeat vpnclient stat reset repeat

The following examples show sample output from the vpnclient stat command. For more information on statistical output, see *VPN Client User Guide for Windows*.

Example 8-8 vpnclient stat Command

Following is an example of the information that the vpnclient stat command displays.

```
C:\Program Files\Cisco Systems\UPN Client>upnclient stat
Cisco Systems UPN Client Version 4.0 (int_92)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.0.2195
UPN tunnel information.
Connection Entry: Engineering
Client address: 200.200.100.50
Server address: 10.10.32.32
Encryption: 168-bit 3-DES
Outhertication: HMAC-MDE
Authentication: HMAC-MD5
IP Compression: None
NAT passthrough is inactive
Local LAN Access is disabled
Personal Firewall: Cisco Systems Integrated Client
Firewall Policy: Centralized Protection Policy (CPP)
UPN traffic summary.
Time connected: 0 day(s), 16:03.25
Bytes in: 60424
Bytes out: 176802
Packets encrypted: 1079
Packets decrypted: 1079
Packets bypassed: 3511
Packets discarded: 17324
Configured routes.
Secured Network Destination
0.0.0.0
                                                                        Netmask
                                                                        0.0.0.0
Firewall Rules.
Act Dir Src Address
Fwd In 10.10.32.32/32
Fwd Out 10.10.032.32/32
Fwd In 10.10.32.32/32
Fwd Out 10.10.0.32/32
                                                                 Dst Address
10.10.0.32/32
10.10.32.32/32
10.10.0.32/32
10.10.32.32/32
                                                                                                                             Src Port
                                                                                                                                                          Dst Port
                                                                                                            Pro
                                                                                                              17
17
                                                                                                                                        500
                                                                                                                                                                    500
500
                                                                                                                                        500
                                                                                                               50
                                                                                                                                                                    Any
                                                                                                                                         Any
                                                                                                               50
                                                                                                                                         Any
                                                                                                                                                                    Aný
N∕A
                     Any
200.200.100.50/32
Fwd
           Ιn
                                                                 200.200.100.50/32
                                                                                                             Any
                                                                                                                                                                    N∕A
N⁄A
Fwd
           Out
                                                                 Any
                                                                                                             Any
                                                                                                                                         N/A
           Out
                                                                                                                                         N/A
Fwd
                      Local
                                                                 Anv
                                                                                                             Anv
Drp
           Ιn
                      Any
                                                                 Local
                                                                                                             Anv
           Out
                      Local
                                                                 Any
```

Example 8-9 vpnclient stat reset Command

The vpnclient stat reset command resets all connection counters.

```
C:\Program Files\Cisco Systems\UPN Client>upnclient stat reset
Cisco Systems UPN Client Version 4.0 (int_92)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.0.2195
```

Tunnel statistics have been reset.

3505

Example 8-10 vpnclient stat traffic Command

Here is a sample of the information that the vpnclient stat traffic command generates.

```
C:\Program Files\Cisco Systems\UPN Client\vpnclient stat traffic Cisco Systems UPN Client Uersion 4.0 (int_92)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.0.2195

UPN traffic summary.
Time connected: 0 day(s), 16:05.28
Bytes in: 60928
Bytes out: 178080
Packets encrypted: 1088
Packets decrypted: 1088
Packets bypassed: 3517
Packets discarded: 17392
```

Example 8-11 vpnclient stat tunnel Command

To display only tunneling information, use the vpnclient stat tunnel command. Here is a sample.

```
C:\Program Files\Cisco Systems\UPN Client>vpnclient stat tunnel
Cisco Systems UPN Client Uersion 4.0 (int_92)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.0.2195

UPN tunnel information.
Connection Entry: Engineering
Client address: 200.200.100.50
Server address: 10.10.32.32
Encryption: 168-bit 3-DES
Authentication: HMAC-MD5
IP Compression: Mone
NAT passthrough is inactive
Local LAN Access is disabled
Personal Firewall: Cisco Systems Integrated Client
Firewall Policy: Centralized Protection Policy (CPP)
```

Example 8-12 vpnclient stat route Command

The vpnclient stat route command displays information similar to the following display.

```
C:\Program Files\Cisco Systems\UPN Client>vpnclient stat route
Cisco Systems UPN Client Version 4.0 (int_92)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.0.2195

Configured routes.
Secured Network Destination Netmask
0.0.0.0 0.0.0
```

Example 8-13 vpnclient stat firewall Command—Windows Only

The vpnclient stat firewall command displays information similar to the following display.

C:\Program Files\Cisco Systems\UPN Client>upnclient stat firewall Cisco Systems UPN Client Version 4.0 (int_92) Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved. Client Type(s): Windows, WinNT Running on: 5.0.2195

Personal Firewall: Cisco Systems Integrated Client Firewall Policy: Centralized Protection Policy (CPP)

Fire	wall	Rules.				
Act	Dir	Src Address	Dst Address	Pro	Src Port	Dst Port
Fwd	In	10.10.32.32/32	10.10.0.32/32	17	500	500
Fwd	Out	10.10.0.32/32	10.10.32.32/32	17	500	500
Fwd	In	10.10.32.32/32	10.10.0.32/32	50	Any	Any
Fwd	Out	10.10.0.32/32	10.10.32.32/32	50	Any	Any
Fwd	In	Any	200.200.100.50/32	Any	N∕Ā	N∕Ā
Fwd	0ut	200.200.100.50/32	Any	Any	N/A	N∕A
Fwd	Out	Local	Any	Any	N/A	N/A
Drp	In	Any	Local	Any	N∕A	N∕A
Drp	Out	Local	Any	Any	N∕A	N∕A Š
						P~-



The maximum size of any VPN Client statistics count is 4,294,967,296. Once the VPN Client software reaches this limit, the statistics count rolls back to zero and starts again.

Return Codes

This section lists the error levels (return codes) that you can receive when using the VPN Client command-line interface.

Return Code	Message	Meaning
200	SUCCESS_START	The VPN Client connection started successfully.
201	SUCCESS_STOP	The VPN Client connection has ended.
202	SUCCESS_STAT	The VPN Client has generated statistical information successfully.
203	SUCCESS_ENUMPPP	The enumppp command has succeeded. This command lists phone book entries when connecting to the Internet via dial-up.
1	ERR_UNKNOWN	An unidentifiable error has occurred during command-line parsing.
2	ERR_MISSING_COMMAND	Command is missing from command-line input.
3	ERR_BAD_COMMAND	There is an error in the command entered; check spelling.
4	ERR_MISSING_PARAMS	The command-line input is missing required parameter(s).
5	ERR_BAD_PARAMS	The parameter(s) in the command input are incorrect; check spelling.
6	ERR_TOO_MANY_PARAMS	The command-line input contains too many parameters.
7	ERR_NO_PARAMS_NEEDED	The command entered does not require parameters.
8	ERR_ATTACH_FAILED	Interprocess communication error occurred attaching to the generic interface.
9	ERR_DETACH_FAILED	Interprocess communication error occurred detaching from the generic interface.
10	ERR_NO_PROFILE	The VPN Client failed to read the profile.
11	ERR_PWD_MISMATCHED	Reserved
12	ERR_PWD_TOO_LONG	The password contains too many characters. The group password limit is 128 characters; the certificate password limit is 255 characters.
13	ERR_TOO_MANY_TRIES	Attempts to enter a valid password have exceed the amount allowed. The limit is three times.
14	ERR_START_FAILED	The connection attempt has failed; unable to connect.
15	ERR_STOP_FAILED	The disconnect action has failed; unable to disconnect.
16	ERR_STAT_FAILED	The attempt to display connection status has failed.
17	ERR_ENUM_FAILED	Unable to list phonebook entries.

Return Code	Message	Meaning
18	ERR_COMMUNICATION_FAILED	A serious interprocess communication error has occurred.
19	ERR_SET_HANDLER_FAILED	Set console control handler failed.
20	ERR_CLEAR_HANDLER_FAILED	Attempt to clean up after a user break failed.
21	ERR_OUT_OF_MEMORY	Out of memory. Memory allocation failed.
22	ERR_BAD_INTERFACE	Internal display error.
23	ERR_UNEXPECTED_CALLBACK	In communicating with the Connection Manager, an unexpected callback (response) occurred.
24	ERR_DO_NOT_CONTINUE	User quit at a banner requesting "continue?"
25	ERR_GUI_RUNNING	Cannot use the command-line interface when connected through the graphical interface dialer application.
26	ERR_SET_WORK_DIR_FAILED	The attempt to set the working directory has failed. This is the directory where the program files reside.
27	ERR_NOT_CONNECTED	Attempt to display status has failed because there is no connection in effect.
28	ERR_BAD_GROUP_NAME	The group name configured for the connection is too long. The limit is 128 characters.
29	ERR_BAD_GROUP_PWD	The group password configured for the connection is too long. The limit is 128 characters.
30	ERR_BAD_AUTHTYPE	The authentication type configured for the connection is invalid.
31	RESERVED_01	Reserved.
32	RESERVED_02	Reserved.
33	ERR_COMMUNICATION_TIMED_OUT	Interprocess communication timed out.
34	ERR_BAD_3RD_PARTY_DIAL	Failed to launch a third-party dialer.
35	ERR_DAEMON_NOT_RUNNING (CVPND.EXE)—Non-Windows only	Connection needs to be established for command to execute.
36	ERR_DAEMON_ALREADY_RUNNING (CVPND.EXE)—Non-Windows only	Command cannot work because connection is already established.

Application Example—Windows Only

Here is an example of a DOS batch file (.bat) that uses CLI commands to connect to the corporate office from a branch office, run an application, and then disconnect from the corporate site.

```
runxls.bat
rem assume you have generated a report in the middle of the night that needs
rem to be sent to the corporate office.
rem .. generate report.xls . .
rem connect to the home office
vpnclient connect myprofile user admin pwd admin
rem check return code from vpnclient call....
if %errorlevel% neq 200 goto failed
rem if okay continue and copy report
copy report.xls \\mycorpserver\directory\overnight_reports /v
rem now disconnect the VPN connection
vpnclient disconnect
echo Spreadsheet uploaded
goto end
:failed
echo failed to connect with error = %errorlevel%
:end
```

Application Example—Windows Only



CHAPTER 9

Managing Digital Certificates from the Command Line

This chapter describes how use the command-line interface to manage digital certificates in your certificate store. Your certificate store is the location in your local file system for storing digital certificates. The store for the VPN Client is the Cisco store.

Setting Certificate Keywords

To use certificates for authentication, you must correctly set all keywords that apply to certificates in your user profile. Check your settings for the following keywords:

- **AuthType = 3** (certificate authentication)
- **CertStore** = **1** (Cisco certificate store)
- CertName = Common Name (This must be the same common name entered for a certificate.)

For more information on setting parameters in your user profile, see "User Profiles, page 5-1."

Certificate Command Syntax

The command line interface for certificate management operates in two ways:

• The standard UNIX shell or the DOS command-line prompt at which you enter all arguments for a given command on the same line.

```
{\tt cisco\_cert\_mgr~-U~-op~enroll~-f~} {\it filename~-chall~challenge\_phrase}
```

• A prompting mode in which you enter minimum arguments for a given command and are prompted for any remaining information.

The minimum command line argument follows this basic form:

```
cisco_cert_mgr -U -op operation
cisco_cert_mgr -R -op operation
cisco_cert_mgr -E -op operation
```

Where:

- **- U** applies to the user or private certificate.

You can use the -U flag for all certificate management command operations, except enroll_resume.

- **R** applies to the root certificate or certificate authority (CA) certificate.

You can use the -R flag for list, view, verify, delete, export, import, and change password operations.

- **E** applies to certificate enrollment.

You can only use the -E flag with list and delete, and you must specify it using the enroll_resume operation.

The operation for the specified certificate follows the **-op** argument. Valid operations for the certificate manager command are list, view, verify, delete, export, import, enroll, enroll_file, and enroll_resume. For more information on these operations, see the "Certificate Management Operations."

For example, if you enter the following command:

```
cisco-cert-mgr -R -op import
```

Certificate manager prompts you for the name of the file to import.

Certificate Contents

This section describes the type of information contained in a digital certificate.

A typical digital certificate contains the following information:

- Common name—The name of the owner, usually both the first and last names. This field identifies the owner within the Public Key Infrastructure (PKI) organization.
- Department—The name of the owner's department. This is the same as the organizational unit.
 - If you are connecting to a VPN 3000 Concentrator, this field must match the **Group Name** configured for the owner in the device.
- Company—The company in which the owner is using the certificate. This is the same as the
 organization.
- State—The state in which the owner is using the certificate.
- Country—The two-character country code in which the owner's system is located.
- Email—The e-mail address of the owner of the certificate.
- Thumbprint—An MD5 hash of the certificate's complete contents. The thumbprint provides a means for validating the authenticity of the certificate. For example, if you contact the issuing CA, you can use this identifier to verify that this certificate is the correct one to use.
- Key size—The size of the signing key pair in bits.
- Subject—The fully qualified domain name (FQDN) of the certificate's owner. This field uniquely identifies the owner of the certificate in a format that can be used for LDAP and X.500 directory queries. A typical subject includes the following fields:
 - common name (cn)
 - organizational unit, or department (ou)
 - organization or company (o)
 - locality, city, or town (l)
 - state or province (st)
 - country (c)
 - e-mail address (e)

Other items might be included in the Subject, depending on the certificate.

- Serial number—A unique identifier used for tracking the validity of the certificate on the certificate revocation lists (CRLs).
- Issuer—The FQDN of the source that provided the certificate.
- Not before—The beginning date that the certificate is valid.
- Not after—The end date beyond which the certificate is no longer valid.

The following output is an example of the type of information contained in a digital certificate:

```
Common Name: Fred Flintstone
Department: Rock yard
Company: Stone Co.
State: (null)
Country: (null)
Email: fredf@stonemail.fake
Thumb Print: 2936A0C874141273761B7F06F8152CF6
Key Size: 1024
Subject:e=fredf@stonemail.fake,cn=Fred Flinstone,ou=Rockyard,o=Stone Co. l=Bedrock
Serial #: 7E813E99B9E0F48077BF995AA8D4ED98
Issuer: Stone Co.
Not before: Thu May 24 18:00:00 2001
Not after: Mon May 24 17:59:59 2004
```

Certificate Passwords

Each digital certificate is protected by a password. Many operations performed by the certificate management command require that you enter the password before the operation can take place.

The operations that require you to enter a password are:

- · Delete
- Import
- Export
- Enroll



For the enroll operation, the password to protect the digital certificate is a separate password from the optional challenge password that you enter for the server certificate.

You are prompted for any passwords that are required to complete the command. You must enter the password and verify the password again before the command can execute. If the password is not accepted, you must re-enter the command.

When you establish a VPN connection with a certificate, a certificate password is also required.

All passwords can be up to 32 alphanumeric characters in length, and are case sensitive.

Certificate Tags

A certificate tag is the identifier for each unique certificate. Each certificate added to the certificate store is assigned a certificate tag. An enroll operation also generates a certificate tag, even if the enroll operation does not complete.

Some certificate management operations require that you enter a certificate tag argument before the operation can take place. Operations that require certificate tags are listed in Table 9-1. Use the **list** operation to find your certificate tag.

To enter a certificate tag argument, use the **-ct** command followed by the certificate identifier, listed as **-ct** *Cert* # next to the operation.

The following example shows the **view** command with a required certificate tag:

```
cisco cert mgr -U -op view -ct 0
```

Where the operation is view, and the certificate tag is 0.

If you do not enter the **-ct** argument and certificate tag, the command line prompts you for them. If you enter an invalid certificate tag, the command line lists all certificates in the certificate store, and prompts you again for the certificate tag.

Certificate Management Operations

List all certificate management operations on the command line following the minimum command line argument. Valid operation strings allow you to list, view, verify, delete, export, import, and enroll digital certificates in your store.

The following is an example of a certificate management command with the **list** operation, and a sample output.

Table 9-1 describes the operations that can be used with the certificate management command.

Table 9-1 Parameters for the cert_mgr Command

Parameter	Description	
	Lists all certificates in the certificate store. Each certificate in the list is identified by a unique certificate tag (<i>Cert #</i>).	
view -ct Cert #	Views the specified certificate. You must enter a certificate tag.	

Table 9-1 Parameters for the cert_mgr Command (continued)

Parameter	Description	
verify -ct Cert #	Verifies that the specified certificate is valid. You must enter a certificate tag.	
	If the certificate is verified, the message 'Certificate <i>Cert</i> # verified' appears.	
	If the certificate fails verification for any reason, the message 'Certificate <i>Cert</i> # failed verification' appears. Following this message is a text string that describes the reason for the failure.	
delete -ct Cert #	Deletes the specified certificate. You must enter a certificate tag.	
export -ct Cert # -f filename	Exports the identified certificate from the certificate store to a specified file. You must enter a certificate tag and a filename. If you omit either, the command line prompts you for them.	
	You must enter the full path of the destination. If you enter only the filename, the file is placed in your working directory.	
	Exporting a certificate	
	You might want to export a certificate, primarily for backing up your certificate and private key or for moving them to another system. When you export a certificate, you are making a copy of it.	
	Certificates are exported in a Cisco proprietary format that can be imported only by another Cisco VPN Client.	
import -f filename	Imports a certificate from a specified file to the certificate store.	
	This operation requires two different passwords: the password that protects the file (assigned by your administrator), and the password you select to protect the certificate.	
	Certificates must be in one of the following formats and must contain the private key in order for the Windows VPN Client to import the certificate:	
	• PKCS#12 (.PFX)	
	• PKCS#7 (P&B)	
	• X.509 (.CER)	
enroll	For user certificates only.	
-cn common_name -ou organizational_unit	Obtains a certificate by enrolling you with a Certificate Authority (CA) over the network.	
-o organization -st state	Enter each keyword individually on the command line.	
-c country	See the "Enrolling Certificates" for more information.	
-e email	You can obtain a challenge phrase from your administrator or from	
-ip IP_Address -dn domain_name -caurl url_of _CA -cadn domain_name	the CA.	
[-chall challenge_phrase]		

Table 9-1 Parameters for the cert_mgr Command (continued)

Parameter	Description	
enroll_file -cn common_name	For user certificates only.	
-ou organizational_unit -o organization -st state	Generates an enrollment request file that you can e-mail to the CA or paste into a webpage form. When CA generates the certificate, you must import it using the import operation.	
-c country -e email -ip IP_Address -dn domain_name -f filename -enc [base64 binary]	See the "Enrolling Certificates" for more information.	
enroll_resume -E -ct Cert #	You cannot use this operation with user or root certificates. Resumes an interrupted network enrollment. You must enter the -E argument and a certificate tag.	
changepassword -ct Cert #	Changes a password for a specified digital certificate. You must enter a certificate tag. You must enter the current password before you select the new password and confirm it.	

Enrolling Certificates

A Certificate Authority (CA) is a trusted organization that issues digital certificates to users for verifying that they are who they claim to be. The certificate enrollment operations allow you to obtain your certificate from a CA over the network or from an enrollment request file.

There are three types of certificate enrollment operations.

- The **enroll** operation allows you to obtain a certificate by enrolling with a CA over the network. You must enter the URL of the CA, the domain name of the CA, and the common name.
- The **enroll_file** operation generates an enrollment request file that you can e-mail to a CA or post into a webpage form. You must enter a filename, a common name, and an encoding type.
 - With the enroll and enroll_file operations, you can include keywords to supply additional information (see Table 9-2).
- The **enroll_resume** operation resumes an interrupted network enrollment. You must enter the **-E** argument and a certificate tag. To find your certificate tag, use the **list** operation.

Enrollment Operations

To use enrollment operations, enter the certificate manager command, an enroll operation, and the associated keywords on the command line.

• The following example shows the enroll command with the minimum required keywords for common name (-cn), URL of the CA (-caurl) and domain name of the CA (-cadn):

```
cisco_cert_mgr -U -op enroll -cn Ren Hoek -caurl
http://172.168.0.32/certsrv/mscep/mscep.dll -cadn nobody.fake
```

• The following example shows the enroll_file command with the minimum required keywords for filename (-f), common name (-cn), and encoding type (-enc):

```
cisco_cert_mgr -U -op enroll_file -f filename -cn Ren Hoek -enc base64
```

 The following example shows the enroll_file command with the required minimum arguments and additional keywords:

```
cisco_cert_mgr -U -op enroll_file -f filename -cn Ren Hoek -ou Customer Service -o Stimpy, Inc, -st CO -c US -e ren@fake.fake -ip 10.10.10.10 -dn fake.fake -enc binary
```

• The following example shows the enroll_resume command:

```
cisco_cert_mgr -E -op enroll_resume -ct 4
```

Table 9-2 describes options for the enroll, enroll_file, and enroll_resume operations.

Table 9-2 Keywords for Enrollment Operations

Parameter	Description	
-cn common_name	The common name for the certificate.	
-ou organizational_unit	The organizational unit for the certificate.	
-o organization	The organization for the certificate.	
-st state	The state for the certificate.	
-c country	The country for the certificate.	
-e email	The user e-mail address for the certificate.	
-ip IP_Address	The IP address of the user's system.	
-dn domain_name	The FQDN of the user's system.	
-caurl url_of_CA	The URL or network address of the CA.	
-cadn domain_name	The CA's domain name.	
[-chall challenge_phrase]	You can obtain the challenge phrase from your administrator or from the CA.	
-enc [base64 binary]	Select encoding of the output file. The default is base64.	
	• base64 is an ASCII-encoded PKCS10 file that you can display because it is in a text format. Choose this type when you want to cut and paste the text into the CA's website.	
	• binary is a base-2 PKCS10 (Public-Key Cryptography Standards) file. You cannot display a binary-encoded file.	

Enrollment Troubleshooting Tip

If the enrollment request for a user certificate, using either the enroll or enroll_file operation, generates a CA certificate instead of a user certificate, the CA might be overwriting some of the distinguished naming information. This might be caused by a configuration issue on the CA, or a limitation of how the CA responds to enrollment requests.

The common name and subject in the enrollment request must match the certificate generated by the CA for the VPN Client to recognize it as the user certificate you requested. If it does not match, the VPN Client does not install the new user certificate as requested.

To check for this problem, view the enrollment request on the VPN Client and compare the common name and subject lines with a view of the certificate from the CA. If they do not match, then the CA is overwriting information from the client request.

To work around this issue, use the invalid certificate as an example and create an enrollment request that matches the output of the CA certificate.



If the CA's certificate contains multiple department (multiple ou fields), you can add multiple departments to the VPN Client enrollment request by using the plus sign (+) between the department fields.



CHAPTER 10

Customizing the VPN Client Software

This chapter explains how to replace the Cisco Systems brand with your own organization's brand. When you install and launch the VPN Client software, you see your own organization name, program name, and application names on menus, windows, dialogs, and icons.

For the Windows platform, it also explains how to set up the software so that your users can install it automatically without being prompted. This feature is called *silent install*.

To customize the VPN Client software, you create your own distribution image combining the following elements, which this chapter describes.

For all platforms, you can customize the following:

- Cisco Systems image that you receive on the Cisco Systems software distribution CD.
- Your own portable network graphics (PNG) (Table 10-1) and icon files to replace the Cisco Systems brand.
- A vpnclient.ini file for configuring the VPN Client software globally (see Chapter 5, "Preconfiguring the VPN Client for Remote Users").
- Individual profile (.pcf) files for each connection entry (see Chapter 5, "Preconfiguring the VPN Client for Remote Users").

Table 10-1 lists the GUI image (portable network graphic) files that the VPN Client uses. If you want to replace any of them with your own image files, you must name your image files exactly as shown in the list; otherwise, the VPN Client GUI does not recognize them.

Table 10-1 Portable Network Graphic Files

PNG File	Description	
splash_screen.png	Splash screen that appears for 2 to 5 seconds when the GUI starts. This screen contains a logo, product name and version, and copyright information.	
	Rebranded splash-screen graphics must be at least 280 pixels wide to accommodate the box that displays the status text. There must be a full-width blank area at the bottom of the graphic at least 36 pixels in height.	
title_bar.png	Image at the left end of the title bar	
connected.png	Image next to connection entry when connection is active	
logo.png	Organization logo for simple and advanced mode main dialogs	

Table 10-1 Portable Network Graphic Files (continued)

PNG File	Description	
password_logo.png	Organization logo for password dialog (XAuth), group name and password)	
profile_logo.png	Organization logo for new/modify profile dialog	
status_down_arrow.png	Down arrow on the status bar of advanced mode, used to change the status bar display	
cancel.png	Cancel button on advanced mode connection entries toolbar	
connect_pressed.png	Connect button pressed on advanced mode connection entries toolbar	
disconnect.png	Disconnect button on advanced mode connection entries toolbar	
disconnect_pressed.png	Disconnect button pressed on advanced mode connection entries toolbar	
new_profile.png	New button on advanced mode connection entries toolbar	
new_profile_pressed.png	New button pressed on advanced mode connection entries toolbar	
import_profile.png	Import button on advanced mode connection entries toolbar	
import_profile_pressed.png	Import button pressed on advanced mode connection entries toolbar	
modify_profile.png	Modify button on advanced mode connection entries toolbar	
modify_profile_pressed.png	Modify button pressed on advanced mode connection entries toolbar	
delete_profile.png	Delete button on advanced mode connection entries toolbar	
delete_profile_pressed.png	Delete button pressed on advanced mode view certificates toolbar	
import_certificate.png	Import button on advanced mode view certificates toolbar	
import_certificate_pressed.png	Import button pressed on advanced mode view certificates toolbar	
export_certificate.png	Export button on advanced mode view certificates toolbar	
export_certificate_pressed.png	Export button pressed on advanced mode view certificates toolbar	
delete_certificate.png	Delete button on advanced mode view certificates toolbar	
delete_certificate_pressed.png	Delete button pressed on advanced mode view certificates toolbar	
enroll_certificate.png	Enroll button on advanced mode view certificates toolbar	
enroll_certificate_pressed.png		
verify_certificate.png	Verify button on advanced mode view certificates toolbar	
erify_certificate_pressed.png		
show_certificate.png	ificate.png Show button on advanced mode view certificates toolbar	
show_certificate_pressed.png	Show button pressed on advanced mode view certificates toolbar	
enable_log.png	Enable button on advanced mode connection entries toolbar	
enable_log_pressed.png	d.png Enable button pressed on advanced mode view log toolbar	
disable_log.png	Disable button on advanced mode view log toolbar	
disable_log_pressed.png	Disable button pressed on advanced mode view log toolbar	
clear_log.png	Clear button on advanced mode view log toolbar	

Table 10-1 Portable Network Graphic Files (continued)

PNG File	Description	
clear_log_pressed.png	Clear button pressed on advanced mode view log toolbar	
options_log.png	Options button on advanced mode view log toolbar	
options_log_pressed.png	Options button pressed on advanced mode view log toolbar	
show_log.png	Show button on advanced mode view log toolbar	
show_log_pressed.png	Show button pressed on advanced mode view log toolbar	
arrow_up.png	Up Arrow button in Backup Servers tab of the new/modify profile dialog	
arrow_down.png	Down Arrow button in Backup Servers tab of the new/modify profile dialog	

You can also replace the following icon files (as long as your icon files have these same names):

- connected.ico—the tray icon when connected (also in resource file for vpngui.exe icon)
- · unconnected.ico—the tray icon when not connected
- · disconnecting.ico—the tray icon when disconnecting

Installing the VPN Client Without User Interaction

This section describes how to produce installation without user interaction for MSI installations. Installing the VPN Client without user interaction is called *silent mode*. In silent mode, no messages or prompts appear on the screen.



You can launch silent installation from the command line by using the **-sd** parameter with the vpnclient.exe command. For example, **vpnclient -sd toVPN**. For information on the vpnclient command, refer to "Configuring Automatic VPN Initiation—Windows Only".

Silent Installation Using MSI

To install the VPN Client without dialogs and messages (user interface) displaying on the screen, you can use either of the two following commands on the command line.

msiexec.exe /q [n|b|r|f] /i vpnclient_setup.msi

or

 $vpnclient_en.exe / q [n|b|r|f]$

Option	What it Displays
q or qn	No user interface. It is advisable to enable logging to determine whether the installation succeeded, since this option eliminates all information including fatal error messages.
qb	The basic user interface, which is a limited progress dialog that Windows Installer generates. It is advisable to enable logging with this option as well.

•	Reduced user interface, similar to the full user interface option, but includes only a subset of all dialogs. For example, this option displays the welcome, license agreement, destination folder, and start dialogs, but does not let the user change the destination folder.	
qf	Full or complete user interface including all dialogs. This is the default setting.	

Launching SetMTU with Silent Installation

The SetMTU utility is automatically launched in silent mode with the value of 1300 for all installed adapters. To disable the SetMTU utility during installation, set the LAUNCHSETMTU property on the command-line to 0. To modify the MTU value, set SETMTUVALUE to *value*. To override the DNE MtuAdjuistment parameter, which is set to 0, set DNEMTUADJUSTMENT to *value*.

For example, to disable SetMTU and set the DNE Mtuadjustment to 144, execute the following command:

vpnclient_setup.msi LAUNCHSETMTU=0 DNEMTUADJUSTMENT=144

For information on the SetMTU utility, see "Changing the MTU Size, page 11-5."

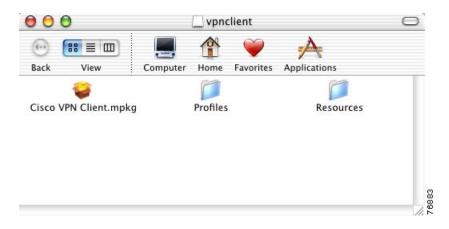
Customizing the VPN Client GUI for Mac OS X

To customize the VPN Client GUI for the Mac OS X platform, place the custom images in the Resources folder of the installer directory.

Figure 10-1shows the vpnclient installer directory. This directory contains the installer package and any preconfigured files in the Profiles and Resources folders.

The Resources folder contains all images for the VPN Client.

Figure 10-1 VPN Client Installer Directory



To distribute custom images, replace the image files in the Resources folder with your own custom images. For example:

- To customize the logo, replace the file /etc/CiscoSystems/Resources/logo.png with your own custom logo.
- To customize the splash screen, replace the file /etc/CiscoSystems/Resources/splash_screen.png with your own custom splash screen.

When the VPN Client is installed, the images in the Resources file are used for the client GUI.

Customizing the VPN Client GUI for Mac OS X



CHAPTER

Troubleshooting and Programmer Notes

This chapter contains information to help you resolve problems installing or running the VPN Client. It also contains notes helpful for writing programs for special needs.

This chapter includes the following main topics:

- Troubleshooting the VPN Client
- Changing the MTU Size
- Delete With Reason
- Start Before Logon and GINAs—Windows Only
- · Programmer Notes
- · IKE Proposals

Troubleshooting the VPN Client

This section describes how to perform the following tasks:

- Gathering VPN Client Logs
- Getting Information About Severity 1 Events
- Gathering System Information for Customer Support
- Solving Common Problems
- · Changing the MTU Size

Gathering VPN Client Logs

The Logs folder in the VPN Client install directory stores log files of VPN Client sessions. Log files are text files with names in the format Log-yyyy-MM-dd-hh-mm-ss.txt. For information on log files and logging, refer to VPN Client User Guide for Windows, Chapter 7 "Managing the VPN Client" or VPN Client User Guide for Mac OS X, Chapter 7, "Managing the VPN Client."

You can obtain these log files for analysis and send them to Customer Support, when necessary.

Getting Information About Severity 1 Events

When severity 1 events occur, the VPN Client logs them in a text file named faultlog.txt. This file exists in the installation directory of the VPN Client. This event logging occurs whether the logviewer application is running or not. For example errors occurring during service initialization cannot be logged to the log viewer, because these errors occur before the service has attached itself to the log viewer. Therefore, you can open the faultlog.txt file to read these severity 1 events. This log file provides a useful tool to help you analyze what is happening and gives you information to report to customer support if you need to contact your customer support representative.

Gathering System Information for Customer Support

If you are having problems running the VPN Client on your PC, you can gather system information that is helpful to a customer support representative and e-mail it to us. We recommend that you do the following *before* you contact us.

If Your Operating System is Windows 98, 98 SE, ME, 2000, or XP

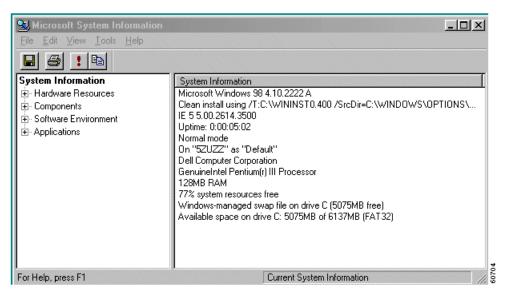


The VPN Client no longer officially supports Windows 95, Windows 98, and Windows ME.

Go to the Start menu and select Programs > Accessories > System Tools > System Information.

Windows displays the Microsoft System Information screen, such as the one in Figure 11-1.

Figure 11-1 System Information Screen on Windows 98



Select a category and the screen displays details for that category. You can then execute the **Export** command and choose a name and destination. Windows creates a text file, which you can attach to an e-mail message and send to the support center.

If Your Operating System is Windows NT or Windows 2000

On the Windows NT or Windows 2000 operating system, you can run a utility named winds from a command-line prompt. WINMSD generates a file containing information about your system configuration, and the software and drivers installed.

To use this utility, perform the following steps:

Step 1 Go to the Start menu and select Programs > Command Prompt.

This action displays a window with a DOS prompt, such as c:\.

Step 2 Type the following command at the DOS prompt:

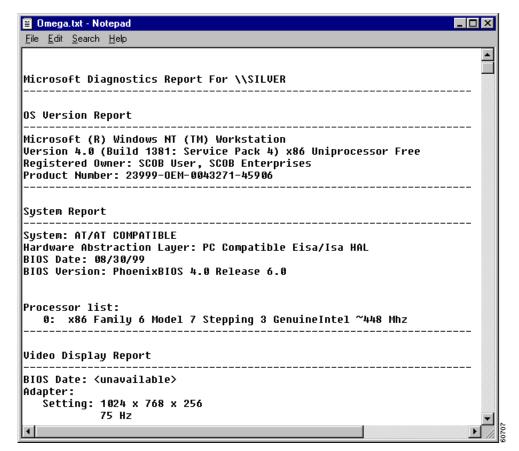
C:\>winmsd/a/f

where /a = all and /f = write to file.

This command generates a text (.txt) file with the name of your computer and places the file in the directory from which you run the command. For example, if the name of your machine is SILVER and you execute the command from the c: drive (as shown above), the text file name is silver.txt.

If you open the file with a text editor, such as Notepad, you see a file such as the one shown in Figure 11-2, which was from a Windows NT system.

Figure 11-2 System Text File



You can attach this file to an e-mail message and send it to the support center.

If Your Operating System is Mac OS X

Step 1 From the command line, execute the following commands:

ifconfig -a uname -a kextstat

Copy the output from the above commands, paste it into an e-mail message, and send it to Support.

Solving Common Problems

This section describes some common problems and what to do about them.

Shutting Down on Windows 98

You may experience a problem with your Windows 98 system shutting down when the VPN Client software is installed. If so, you need to disable the fast shutdown feature, as follows:

- Step 1 At the Microsoft System Information screen (shown in Figure 11-1), select Tools> System Configuration.

 Microsoft displays a Properties page.
- Step 2 From the General page, select the Advanced button.
- Step 3 Choose the Disable Fast Shutdown option.

Booting Automatically Starts up Dial-up Networking on Windows 95

Some versions of Internet Explorer silently control startup options in Windows 95 so that every time you start your system, Dial-Up Networking launches. If this occurs, as it does in Internet Explorer 3.0, go to View > Options > Connections and uncheck the option Connect to the Internet as needed.

Changing the MTU Size

The Set MTU option is used primarily for troubleshooting connectivity problems.



The VPN Client automatically adjusts the MTU size to suit your environment, so running this application is not recommended.

The maximum transmission unit (MTU) parameter determines the largest packet size in bytes that the client application can transmit through the network. If the MTU size is too large, the packets may not reach their destination. Adjusting the size of the MTU affects all applications that use the network adapter. Therefore the MTU setting you use can affect your PC's performance on the network.

MTU sizing affects fragmentation of IPsec and IPsec through NAT mode packets to your connection destination, because IPsec encapsulation increases packet size. A large size (for example, over 1300) can increase fragmentation. Using 1300 or smaller usually prevents fragmentation. Fragmentation and reassembly of packets at the destination causes slower tunnel performance. Also, many firewalls do not let fragments through.

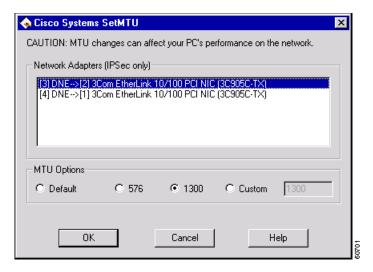
Changing the MTU Size—Windows

To change the size of the MTU for Windows, use the following procedure:

Step 1 Select Start > Programs > Cisco Systems VPN Client > SetMTU.

The Set MTU window appears.

Figure 11-3 Setting MTU Size on Windows NT



- Step 2 Click a network adapter on the list of network adapters.
- Step 3 Click one of the following choices under MTU Options:

Default	The factory setting for this adapter type.
576 (in bytes)	The standard size for dial-up adapters.
1300 (in bytes)	The choice recommended for both straight IPsec and IPsec through NAT. Using this value guarantees that the client does not fragment packets under normal circumstances.
Custom	Enter a value in the box. The minimum value for MTU size is 68 bytes.

Step 4 Click OK.

You must restart your system for your change to take effect.

Changing the MTU Size—Linux, Solaris, and Mac OS X

To change the MTU size:

- Step 1 Open a terminal (Mac OS X-only).
- Step 2 Type the following command:

sudo ifconfig en0 mtu 1200

(Replace the en0 with the appropriate interface, and replace 1200 with the desired mtu.)

Step 3 The changes take effect immediately.

Setting the MTU from the Command Line

You can use the SetMTU command at the command-line prompt to set the MTU size. The syntax of the SetMTU command follows:

setmtu /switch value

where switch can be one of the following:

Switch	Description
/s value	Set the MTU for all adapters to <i>value</i> . This sets the MTU at the IP layer. This action requires a reboot.
/r	Reset the MTU for all adapters to the operating system default at the IP layer. This action requires a reboot.
/va value	Set the MTU for the virtual adapter to <i>value</i> . This sets the MTU at the MAC layer. This action does not require a reboot.
/vaReset	Reset the MTU for the virtual adapter to the default (1500) at the MAC layer. This action does not require a reboot.
/?	Display help on the SetMTU switches.

The new setting remains in effect the next time a tunnel is established.

Delete With Reason

When a disconnect occurs, the VPN Client displays a reason code or reason text. The VPN Client supports the delete with reason function for client-initiated disconnects, secure-gateway-initiated disconnects, and IPsec deletes.

- If you are using a GUI VPN Client, a pop-up message appears stating the reason for the disconnect, the message is appended to the Notifications log, and is logged in the IPsec log (Log Viewer window).
- If you are using a command-line client, the message appears on your terminal and is logged in the IPsec log.
- For IPsec deletes, which do not tear down the connection, an event message appears in the IPsec log file, but no message pops up or appears on the terminal.



The secure gateway you are connecting to must be running software version 4.0 or later to support delete with reason functionality.

Table 11-1 describes the reason codes and the corresponding messages.

Table 11-1 Delete with Reason Codes

Reason Code	Translated Text
IKE_DELETE_SERVER_SHUTDOWN	Peer has been shut down
IKE_DELETE_SERVER_REBOOT	Peer has been rebooted.
IKE_DELETE_MAX_CONNECT_TIME	Maximum configured connection time exceeded.

Table 11-1 Delete with Reason Codes

Reason Code	Translated Text
IKE_DELETE_BY_USER_COMMAND	Manually disconnected by administrator.
IKE_DELETE_BY_ERROR	Connectivity to Client lost.
IKE_DELETE_NO_ERROR	Unknown error.
IKE_DELETE_IDLE_TIMEOUT	Maximum idle time for session exceeded.
IKE_DELETE_P2_PROPOSAL_MISMATCH	Policy negotiation failed
IKE_DELETE_FIREWALL_MISMATCH	Firewall policy mismatch.
IKE_DELETE_CERT_EXPIRED	Certificates used with this connection entry have expired.
IKE_DELETE_BY_EXPIRED_LIFETIME	Maximum configured lifetime exceeded.

All text messages for client-initiated disconnects begin with "Secure VPN Connection terminated terminated locally by the client".

All text messages for secure-gateway-initiated disconnects begin with "Secure VPN Connection terminated by Peer X.X.X.X", where X.X.X.X is the IP address of the secure gateway.

The translated reason code or the reason text follows.

Configuring Delete with Reason on a VPN Concentrator

To receive disconnect information from a 4.0 or greater VPN Concentrator, you must configure the feature as follows:

- Step 1 Go to Configuration | Tunneling | IPsec | Alerts
- Step 2 Check Alert when disconnecting.
- Step 3 Click Apply.
- Step 4 Save the configuration.

Start Before Logon and GINAs—Windows Only

The VPN Client can load prior to logging in to a Windows NT platform (Windows NT 4.0, Windows 2000, and Windows XP). This feature lets remote users establish a VPN connection to a private network where they can successfully log in to a domain. When start before logon (SBL) is enabled on a Windows NT platform, the VPN Client tries to replace the standard Microsoft logon dialog box (the same one that appears after you press Ctrl+Alt+Del when booting your PC, called a GINA). The name of the Microsoft GINA is msgina.dll and you can find it in the registry at the location:

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
GinaDLL = msgina.dl1

The VPN Client replaces the msgina.dll with the VPN Client's GINA (csgina.dll), and then points to it so that you can still see and use the MS GINA. When you start your PC and press Ctrl+Alt+Del, you are launching the VPN Client Dialer application and the MS logon dialog box. The VPN Client detects whether the necessary Windows services are running and if not, displays a message asking you to wait.

If you look in the VPN Client registry, you see the following parameters and values:

```
HKLM\Software\Cisco Systems\VPN Client\
GinaInstalled = 1
PreviousGinaPath = msqina.dll
```



When you enable start before logon for the first time, you must reboot for the system to load csgina.

Fallback Mode

In some cases a third-party program replaces the MS GINA, and in some of these cases the VPN Client works with the third-party program, while in other cases, it does not. The VPN Client maintains a list of incompatible GINAs that it does not work with, and does not replace the GINA file in use. This is called *fallback* mode. The list of incompatible GINAs resides in the vpnclient.ini file, and the VPN Client refers to the list only during installation. The following entry is an example.

```
IncompatibleGinas=PALgina.dll,nwgina.dll,logonrem.dll,ngina.dll
```

In fallback mode, the VPN Client performs differently when start before logon is in use. Instead of loading when you press Ctrl+Alt+Del, the VPN Dialer loads as soon as the VPN service starts. When operating in fallback mode, the VPN Client does not check to see if the necessary Windows services have started. As a result, the VPN connection could fail if initiated too quickly. In fallback mode, when the VPN connection succeeds, you then press Ctrl+Alt+Del to get to the Microsoft logon dialog box. In this mode, you see the following VPN Client registry parameters and values:

```
HKLM\Software\Cisco Systems\VPN Client\
GinaInstalled = 0
PreviousGinaPath = msgina.dll
```

Incompatible GINAs

If a new problem GINA is discovered after the VPN Client is released, you can add the GINA to the incompatible GINA list in the vpnclient.ini file. Adding the GINA to this list places it in the IncompatibleGinas list in the registry when you install the VPN Client and puts the VPN Client into fallback mode, thus avoiding possible conflicts (see section Start Before Logon and GINAs—Windows Only, page 11-8).

Disabling the Firewall Dialogs

You can disable firewall dialogs that display to the user during the SBL period when firewalls are not running. The registry key DisableSBLFirewallCheck controls this function.

The registry location is:

HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems\VPN Client\Secure

The key is DisableSBLFirewallCheck, with the following values:

- 0 (FALSE)—Do not disable firewall checking. Firewall dialogs appear to users.
- 1- (TRUE)—Disable firewall checking. Firewall dialogs *do not* appear to users.

Programmer Notes

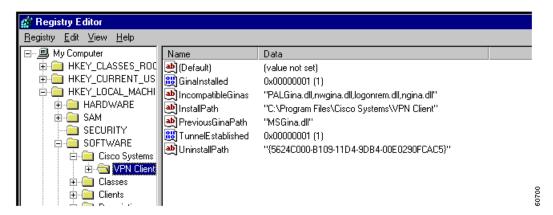
This section contains information to aid a programmer in writing programs that perform routine tasks.

Testing the Connection

As part of a program, you might want to test a connection to see if it is active before performing the tasks that are the purpose of the program. To test the connection, you can poll the TunnelEstablished entry in the HKEY_LOCAL_MACHINE registry.

To see this entry, bring up the Registry Editor and go to SOFTWARE > Cisco Systems > VPN Client. (See Figure 11-4.) In the list of entries, you see TunnelEstablished. This entry can have only two values: 1 or 0. If the connection is working, the value is 1; if not, the value is 0.

Figure 11-4 Cisco Systems VPN Client Registry Entries



Command Line Switches for vpngui Command—Windows Only

The vpngui command starts a connection from the command line by bringing up the VPN Client GUI application. You can use switches to specify parameters with this command. You must precede a switch with a forward slash (/) or hyphen (-). Non-Windows platforms allow only a hyphen prefix.

Table 11-2 lists the switches you can include in the vpngui command and describes the task that each switch performs. If the connection entry name contains spaces or other special characters, you must enclose the name in quotes. In the following examples, towork is the name of the connection entry.

Table 11-2 Command Line Switches

Switch	Parameter	Description	
/c	Auto-connect	Starts the VPN Client application for the specified connection entry and displays the authentication dialog. If no connection entry is specified, then the VPN Client uses the default connection entry. The c and sc switches are mutually exclusive.	
		Example: vpngui /c towork	
/eraseuserpwd	Erase User Password	Erases the user password saved on the Client PC thereby forcing the VPN Client to prompt for a password.	
		Example: vpngui /c /eraseuserpwd towork	
		Note A connection entry may have been configured with Saved Password to suppress a password prompt when connecting using a batch file. Use the eraseuserpwd option to return to require password input from the console when connecting. You cannot combine this switch with the pwd switch. You may use it only with the /c or the /sc switch.	
/user	Username	Specifies a username for authentication. Suppresses the username prompt in authentication dialog. Used with the pwd switch, it suppresses the authentication dialog entirely. Updates the username in the .pcf file. You can use this parameter only with the /c or the /sc switch.	
		Example: vpngui /c /user robron /pwd siltango towork	
		Note If the name supplied is not valid, the VPN Client displays the authentication dialog on a subsequent authentication request.	

Table 11-2 Command Line Switches (continued)

Switch	Parameter	Description	
/pwd	Password	Specifies a password for authentication. Suppresses the password prompt in authentication dialog. Used with the pwd switch, it suppresses the authentication dialog entirely Updates the password in the .pcf file during authentication and then clears the password from the .pcf file. You can use this switch only with the /c or the /sc switch.	
		Example: vpngui /c /user robron /pwd siltango towork	
		Note If the password supplied is not valid, the VPN Client displays the authentication dialog on a subsequent authentication request. After encrypting and using the password for the connection, the VPN Client clears the password in the .pcf file. Using this option on the command line compromises security and is not recommended.	
/sd	Silent disconnect	Suppresses connection terminating messages, such as "You IPsec connection has been terminated." You can use this parameter to improve the automatic connection process. Yo can use this switch only with the /c or the /sc switch.	
		Example: vpngui /sd towork	

IKE Proposals

Table 11-3 lists the IKE proposals that the VPN Client supports.

Table 11-3 Valid VPN Client IKE Proposals

Proposal Name	Authentication Mode	Authentication Algorithm	Encryption Algorithm	Diffie- Hellman Group
CiscoVPNClient-3DES-MD5	Preshared Keys (XAUTH)	MD5/HMAC-128	3DES-168	Group 2 (1024 bits)
CiscoVPNClient-3DES-SHA	Preshared Keys (XAUTH)	SHA/HMAC-160	3DES-168	Group 2 (1024 bits)
CiscoVPNClient-DES-MD5	Preshared Keys (XAUTH)	MD5/HMAC-128	DES-56	Group 2 (1024 bits)
CiscoVPNClient-AES128-MD5	Preshared Keys (XAUTH)	MD5/HMAC-128	AES-128	Group 2 (1024 bits)
CiscoVPNClient-AES128-SHA	Preshared Keys (XAUTH)	SHA/HMAC-160	AES-128	Group 2 (1024 bits)
CiscoVPNClient-AES256-MD5	Preshared Keys (XAUTH)	MD5/HMAC-128	AES-256	Group 2 (1024 bits)
CiscoVPNClient-AES256-SHA	Preshared Keys (XAUTH)	SHA/HMAC-160	AES-256	Group 2 (1024 bits)
IKE-3DES-MD5	Preshared Keys	MD5/HMAC-128	3DES-168	Group 2 (1024 bits)
IKE-3DES-SHA	Preshared Keys	SHA/HMAC-160	3DES-168	Group 2 (1024 bits)
IKE-DES-MD5	Preshared Keys	MD5/HMAC-128	DES-56	Group 2 (1024 bits)
IKE-AES128-MD5	Preshared Keys	MD5/HMAC-128	AES-128	Group 2 (1024 bits)
IKE-AES128-SHA	Preshared Keys	SHA/HMAC-160	AES-128	Group 2 (1024 bits)
IKE-AES256-MD5	Preshared Keys	MD5/HMAC-128	AES-256	Group 2 (1024 bits)
IKE-AES256-SHA	Preshared Keys	SHA/HMAC-160	AES-256	Group 2 (1024 bits)
CiscoVPNClient-3DES-MD5-RSA	RSA Digital Certificate (XAUTH)	MD5/HMAC-128	3DES-168	Group 2 (1024 bits)
CiscoVPNClient-3DES-SHA-RSA	RSA Digital Certificate (XAUTH)	SHA/HMAC-160	3DES-168	Group 2 (1024 bits)
CiscoVPNClient-DES-MD5-RSA-DH1	RSA Digital Certificate (XAUTH)	MD5/HMAC-128	DES-56	Group 1 (768 bits)
CiscoVPNClient-AES128-MD5-RSA	RSA Digital Certificate (XAUTH)	MD5/HMAC-128	AES-128	Group 2 (1024 bits)

Proposal Name	Authentication Mode	Authentication Algorithm	Encryption Algorithm	Diffie- Hellman Group
CiscoVPNClient-AES128-SHA-RSA	RSA Digital Certificate (XAUTH)	SHA/HMAC-160	AES-128	Group 2 (1024 bits)
CiscoVPNClient-AES256-MD5-RSA	RSA Digital Certificate (XAUTH)	MD5/HMAC-128	AES-256	Group 2 (1024 bits)
CiscoVPNClient-AES256-SHA-RSA	RSA Digital Certificate (XAUTH)	SHA/HMAC-160	AES-256	Group 2 (1024 bits)
CiscoVPNClient-3DES-MD5-RSA-DH5	RSA Digital Certificate (XAUTH)	MD5/HMAC-128	3DES-168	Group 5 (1536 bits)
CiscoVPNClient-3DES-SHA-RSA-DH5	RSA Digital Certificate (XAUTH)	SHA/HMAC-160	3DES-168	Group 5 (1536 bits)
CiscoVPNClient-AES128-MD5-RSA-DH5	RSA Digital Certificate (XAUTH)	MD5/HMAC-128	AES-128	Group 5 (1536 bits)
CiscoVPNClient-AES128-SHA-RSA-DH5	RSA Digital Certificate (XAUTH)	SHA/HMAC-160	AES-128	Group 5 (1536 bits)
CiscoVPNClient-AES256-MD5-RSA-DH5	RSA Digital Certificate (XAUTH)	MD5/HMAC-128	AES-256	Group 5 (1536 bits)
CiscoVPNClient-AES256-SHA-RSA-DH5	RSA Digital Certificate (XAUTH)	SHA/HMAC-160	AES-256	Group 5 (1536 bits)
CiscoVPNClient-3DES-MD5-RSA	RSA Digital Certificate (XAUTH)	MD5/HMAC-128	3DES-168	Group 2 (1024 bits)
HYBRID-3DES-SHA-RSA	RSA Digital Certificate (HYBRID)	SHA/HMAC-160	3DES-168	Group 2 (1024 bits)
HYBRID-DES-MD5-RSA-DH1	RSA Digital Certificate (HYBRID)	MD5/HMAC-128	DES-56	Group 1 (768 bits)
HYBRID-AES128-MD5-RSA	RSA Digital Certificate (HYBRID)	MD5/HMAC-128	AES-128	Group 2 (1024 bits)
HYBRID-AES128-SHA-RSA	RSA Digital Certificate (HYBRID)	SHA/HMAC-160	AES-128	Group 2 (1024 bits)
HYBRID-AES256-MD5-RSA	RSA Digital Certificate (HYBRID)	MD5/HMAC-128	AES-256	Group 2 (1024 bits)
HYBRID-AES256-SHA-RSA	RSA Digital Certificate (HYBRID)	SHA/HMAC-160	AES-256	Group 2 (1024 bits)
HYBRID-3DES-MD5-RSA-DH5	RSA Digital Certificate (HYBRID)	MD5/HMAC-128	3DES-168	Group 5 (1536 bits)
HYBRID-3DES-SHA-RSA-DH5	RSA Digital Certificate (HYBRID)	SHA/HMAC-160	3DES-168	Group 5 (1536 bits)
HYBRID-AES128-MD5-RSA-DH5	RSA Digital Certificate (HYBRID)	MD5/HMAC-128	AES-128	Group 5 (1536 bits)
HYBRID-AES128-SHA-RSA-DH5	RSA Digital Certificate (HYBRID)	SHA/HMAC-160	AES-128	Group 5 (1536 bits)
HYBRID-AES256-MD5-RSA-DH5	RSA Digital Certificate (HYBRID)	MD5/HMAC-128	AES-256	Group 5 (1536 bits)

Proposal Name	Authentication Mode	Authentication Algorithm	Encryption Algorithm	Diffie- Hellman Group
HYBRID-AES256-SHA-RSA-DH5	RSA Digital Certificate (HYBRID)	SHA/HMAC-160	AES-256	Group 5 (1536 bits)
IKE-3DES-MD5-RSA	RSA Digital Certificate	MD5/HMAC-128	3DES-168	Group 2 (1024 bits)
IKE-3DES-SHA-RSA	RSA Digital Certificate	SHA/HMAC-160	3DES-168	Group 2 (1024 bits)
IKE-AES128-MD5-RSA	RSA Digital Certificate	MD5/HMAC-128	AES-128	Group 2 (1024 bits)
IKE-AES128-SHA-RSA	RSA Digital Certificate	SHA/HMAC-160	AES-128	Group 2 (1024 bits)
IKE-AES256-MD5-RSA	RSA Digital Certificate	MD5/HMAC-128	AES-256	Group 2 (1024 bits)
IKE-AES256-SHA-RSA	RSA Digital Certificate	SHA/HMAC-160	AES-256	Group 2 (1024 bits)
IKE-DES-MD5-RSA-DH1	RSA Digital Certificate	MD5/HMAC-128	DES-56	Group 1 (768 bits)
IKE-3DES-MD5-RSA-DH5	RSA Digital Certificate	MD5/HMAC-128	3DES-168	Group 5 (1536 bits)
IKE-3DES-SHA-RSA-DH5	RSA Digital Certificate	SHA/HMAC-160	3DES-168	Group 5 (1536 bits)
IKE-AES128-MD5-RSA-DH5	RSA Digital Certificate	MD5/HMAC-128	AES-128	Group 5 (1536 bits)
IKE-AES128-SHA-RSA-DH5	RSA Digital Certificate	SHA/HMAC-160	AES-128	Group 5 (1536 bits)
IKE-AES256-MD5-RSA-DH5	RSA Digital Certificate	MD5/HMAC-128	AES-256	Group 5 (1536 bits)
IKE-AES256-SHA-RSA-DH5	RSA Digital Certificate	SHA/HMAC-160	AES-256	Group 5 (1536 bits)

Table 11-4 lists phase 2 proposals that the VPN Client sends.

Table 11-4 Phase 2 Proposals

AES256	MD5	IPCOMPRESSION
AES256	SHA	IPCOMPRESSION
AES128	MD5	IPCOMPRESSION
AES128	SHA	IPCOMPRESSION
AES256	MD5	
AES256	SHA	
AES128	MD5	
AES128	SHA	
3DES	MD5	IPCOMPRESSION
3DES	SHA	IPCOMPRESSION
3DES	MD5	
3DES	SHA	
DES	MD5	IPCOMPRESSION
DES	MD5	
NULL	MD5	
NULL	SHA	

VPN Client Application Program Interface

The VPN Client software includes an API that customers can use to perform VPN Client tasks without using the standard command-line or graphical interfaces that Cisco provides. The API comprises a shared library that programmers can link into their application, which allows it to:

- · Connect and disconnect VPN tunnels
- · Authenticate users
- · Receive notifications when tunnels open and close
- · Retrieve tunnel statistics, such as byte and packet counts

The API comes with a programmer's user guide *VPN Client: API Overview*. This guide contains information enabling a programmer not familiar with the code base to use the API. The programmer's guide describes functions and data types, an overview of how to accomplish specific tasks, and easy to follow example programs.



CHAPTER 12

Windows Installer (MSI) Information

This chapter describes how to use the Microsoft Windows Installer for the network administrator. For end user instructions, see *Cisco VPN Client for Windows User Guide*, Chapter 2. For information on customizing the VPN Client applications, see Customizing the VPN Client Using an MSI Transform, page 10-3. For installing MSI without user interaction, see "Installing the VPN Client Without User Interaction, page 10-3."

This chapter includes the following main topics:

- Characteristics of MSI
- Starting the VPN Client MSI
- Logging During Installation

Characteristics of MSI

The following list summarizes the characteristics of MSI installation relevant to the VPN Client:

- · Supported on Windows NT SP6, Windows 2000, Windows XP, and Windows Vista.
- Detects but does not automatically uninstall an older VPN Client. Remove previous versions via Add/Remove programs.
- Provides a standard installation package and customizing process.
- Silent installation can be customized to include error reporting.
- Provides automatic rollback in case of installation failure; undoes changes to the system made during attempted installation.
- Automatic replacement of deleted or corrupted files upon first use. Replaces registry keys associated with shortcuts under Start | Program Files.

Starting the VPN Client MSI

Installing the VPN Client, release 4.0 or higher, via MSI requires Windows Installer version 2.0, which is standard with Windows XP but not with Windows NT 4.0 (SP6) or Windows 2000. When using MSI to install the VPN Client on Windows NT and Windows 2000, the installation application installs or upgrades Windows Installer to version 2.0 or higher. This occurs only once.

To install the VPN Client, you must be an administrator or a restricted user with elevated privileges. However, for the restricted user with elevated privileges, the installation program adds the VPN Client to the Program Menu for only the user that installed the VPN Client, not for all users.

Alternative Ways to Launch MSI

There are various ways to launch MSI. Cisco VPN Client User Guide for Windows explains how to install the VPN Client using an executable that runs a wizard (vpnclient_en.exe). This method automatically installs or upgrades the Windows Installer to version 2.0 if necessary. However, this is only one way to install the application.

Launching MSI via Command Line

If Windows Installer 2.0 is already installed, you can install the VPN Client using the msiexec.exe command on the command line as follows.

msiexec.exe /i vpnclient_en.msi [options]

where

/i is the installation switch.

vpnclient_en.msi is the application to be installed.



For complete documentation on the msiexec.exe command, see *Windows Installer version 2.0*, Microsoft Platform SDK, August 2001.

Launching MSI via the MSI Icon

If Windows Installer is already installed, you can launch the installation package by double-clicking the MSI icon.

Figure 12-1 MSI icon



Logging During Installation

To better understand what is happening while MSI is installing the VPN Client, you should initiate logging on the command line by executing the msiexec.exe command with the following options:

msiexec.exe /l [i|w|e|a|r|u|c|m|o|p|v|+|!|*] logfile

where:

/I is the switch that turns on logging.

logfile is the name of the file to receive the logging information.

Example 12-1 Installing with Logging

Option	Information Provided
i	Status messages
w	Non-fatal warnings
e	All error messages
a	Start up actions
r	Action-specific records
u	User requests
c	Initial user interface parameters
m	Out-of-memory or fatal exit information
0	Out-of-disk-space messages
p	Terminal properties
v	Verbose output
+	Append to existing file
!	Send each line to the log
*	Log all information except for what the verbose option generates.

The following command installs the VPN Client and includes a log of all information (*v). It also specifies sending each line to the log file (!).

msiexec /i vpnclient_en.msi /l*v! vpnclient_msi.log

Example 12-2 Installing via the Executable from the Command Line with Logging

The following command installs the VPN Client and logs all information to a log file.

vpnclient_en.exe /l*v! vpnclient_msi.log



You should always include the ! option for logging, since many of the installer events are not recorded if you do not include this option.

Logging During Installation



INDEX

^	parameters 7-1
A	automatic browser configuration 1-22
activating an IKE proposal 4-5	configuring on VPN Concentrator 1-22, 4-22
adding an SA 4-5	autoupdating VPN Client software
AES 11-13	creating configuration file 6-5
aggressive mode connections, disabling inbound 1-15	creating profile distribution package 6-6
alerting peers before disconnecting 1-15	enabling on VPN Concentrator 6-3
API 11-16	how it works 6-7
AppendOriginalSuffix Option parameter 5-21	managing 6-3
ApplicationLauncher parameters 5-11	Windows 2000 and Windows XP 6-2
Application Program Interface 11-16	AYT firewall policy 1-19, 4-11
attribute-value pairs (AVP) 3-11	
authenticaation	
mutual 1-13	В
authenticating, smart card 1-12	backup server attributes, group policy 3-23
authentication	BackupServer parameter (.pcf file) 5-28
mutual group	backup servers
authentication types 4-26	configured on VPN Concentrator for VPN Client 4-2
types 5-25	Baltimore Technologies 4-9, 5-14
authentication parameters (.pcf file) 5-27	banner message, group policy 3-19
AuthType parameter (.pcf file) 5-25	BlackIce Defender
auto initiation 7-5	firewall on remote PC 1-19, 4-11
AutoInitiationEnable (vpnclient.ini) 5-6, 7-3	Black Ice firewall 3-26
AutoInitiationList (vpnclient.ini) 5-7, 7-3	bluetooth, unsupported 1-3
AutoInitiationRetryInterval (vpnclient.ini) 7-3	browser, automatic configuration 1-22
AutoInitiationRetry IntervalType (vpnclient.ini) 5-7	browser proxy configuration 1-22, 4-22
AutoInitiationRetryIntervalType (vpnclient.ini) 7-3	bypassing DHCP server 5-8
AutoInitiationRetry Limit (vpnclient.ini) 5-7	bypassing installation of firewall files 1-5
configuring 7-1	
connect parameter 7-3	
creating in vpnclient.ini file 7-3	С
examples 7-4	Centralized Protection Policy (CPP) 1-18, 4-11
excluding networks from 7-3	certificate

connecting 4-9, 5-14	Client Update 6-3
contents 9-2	client update on VPN Concentrator 6-3
enrolling a CA 9-6	client upgrade, rebootless 1-4
enrollment 9-2	command-line interface
PKI 4-9, 5-15	error messages 8-11
example 9-3	minimum argument 9-1
management 9-1	command-line switches
management operations 9-4	vpngui 11-10
passwords 9-3	commands
root 9-2	msiexec 10-7, 12-2
store 9-1	logging options 12-3
tags 9-4	vpnclient
user 9-1	connect 8-2
certificate, Entrust 1-10	disconnect 8-6
Certificate Authorities (CA)	displaying a list 8-1
supported 4-9, 5-14	notify 8-5
certificates	stat 8-7
enrollment	verify autoinitconfig 8-5
IP address 5-10	vpngui
parameters (vpnclient.ini) 5-9	command-line switches 11-10
Entrust 1-10, 4-23	company logo
group name requirement 4-5	logo.png 10-1
organization unit field 4-5	compression, IP 11-13
parameters (.pcf files) 5-29	configuration parameters
VPN Client connections	global profile 5-3
configuring VPN concentrator 4-4	individual profiles 5-25
change password operation 9-6	configurations
changing method of initializing VA 5-8	client/server 4-16
changing the MTU size 11-5	configuring
Cisco Integrated Client	auto initiation 7-1
scenario 4-13	backup servers for VPN Client 4-21
VPN Client software 1-18, 4-10	browser proxy 1-22, 4-22
Cisco Integrated Firewall 3-25	Entrust certificate 1-10, 4-23
Cisco Security Agent 3-26	local LAN access for VPN Client 1-20, 4-20
firewall on the remote PC 1-19, 4-11	NAT-T 4-22
client/server firewall 1-19, 4-11	personal firewalls 1-17, 4-9
client access rules, group policy 3-27	RADIUS SDI authentication 5-21
client firewall 1-17	connected.png
client firewall, group policy 3-25	lock image on active connection entry 10-1

connecting from command line	group policy 3-11			
vpngui command 11-10	remote access tunnel group, configuring 3-4			
connection	default connection entry			
ending 8-6	connect on open 5-8			
getting status 8-7	default user profile 5-18			
profiles 5-22	defining rules for firewalls 4-15			
starting with vpnclient command 8-2	delete operation 9-5			
testing 11-9	DES 11-13			
connection entry	Description parameter (.pfc file) 5-25			
default 5-18	DfltGrpPolicy 3-12			
features controlled 5-23	DH1 11-13			
file 5-24	DH5 11-13			
preconfigured	DHCP inbound traffic			
distributing 5-33	stateful firewall 1-18, 4-10			
sample .pcf file 5-23	DHCP Intercept, configuring 3-22			
connection-specific DNS suffix 5-20	DHCP server			
connect on open	bypassing 5-8			
activating 5-18	DHGroup parameter (.pcf files) 5-30			
ConnectOnOpen (vpnclient.ini) 5-8	DialerDisconnect parameter (vpnclient.ini) 5-6			
continuous display (stat command) 8-7	directory			
CPP	profiles 5-2, 5-22			
defining filters and rules 4-15	Disable Fast Shutdown option 11-5			
creating 10-3	disconnecting, alerting peers 1-15			
connection profiles 5-22	displaying			
Entrust profile 1-10, 4-23	information continuously 8-7			
global profile 5-2	notifications 8-5			
IPSec group in VPN Concentrator 4-3	route information 8-7			
MSI transform 10-3	distributing new profiles 6-6			
user profiles in VPN Concentrator 4-4	distributing preconfigured software 5-33			
custom firewall 3-26	DNS parameters 5-11			
customizing the VPN Client GUI for Mac OS X 10-8	DNS suffix			
customizing VPN Client software 10-1	connection-specific 5-20			
for MSI 10-3	primary 5-19			
	Windows platforms 5-19			
	documentation			
D	additional 1-xii			
data formats 1-xvii	cautions 1-xvii			
default	notes 1-xvii			
domain name, group policy 3-21	domain attributes, group policy 3-21			

E	faultlog.txt file 11-2			
A CONTRACTOR OF STREET	files			
elevated privileges (installing MSI) 12-1	.pcf 5-22			
EnableBackup parameter (.pcf file) 5-28	.png 10-1			
EnableISPConnect parameter (.pcf file) 5-26	vpnclient.ini 5-2			
EnableLocalLAN parameter (.pcf file) 5-29	sample 5-3			
EnableLog parameter (vpnclient.ini) 5-6	filters			
EnableNat parameter (.pcf file) 5-28	defining for CPP 4-15			
EnableSplitDNS parameter (.pfc file) 5-31	firewall			
encGroupPwd parameter (.pcf file) 5-26	Black Ice 3-26			
ending a connection 8-6	Cisco Integrated 3-25			
enroll file operation 9-6	Cisco Security Agent 3-26			
enrolling	CPP 1-18			
in a PKI 4-9, 5-15	custom 3-26			
enrolling a CA for certificates 9-2, 9-6	Network Ice 3-26			
enrollment keywords 9-7	none 3-26			
enroll operation 9-5	Sygate personal 3-26			
enroll resume operation 9-6	Zone Labs 1-18, 3-26			
Entrust	firewall, personal 1-17			
Technologies 4-9, 5-15	firewall files, bypassing installation 1-5			
Entrust certificates	firewall information 8-7			
enabling VPN Client 1-10, 4-23	firewall policy, group policy 3-25			
Entrust Entelligence certificate 1-10	firewalls			
EntrustIni parameter (vpnclient.ini) 5-5	AYT 1-19, 4-11			
error messages 8-11	BlackIce Defender 1-19, 4-11			
errors	Cisco Integrated Client 1-18, 4-10			
reporting	Cisco Security Agent 1-19, 4-11			
faultlog.txt file 11-2	client/server			
ESP inbound traffic	configuring 4-16			
stateful firewall 1-18, 4-10	configurations			
events	group 4-16			
severity 1	matching 1-18, 4-10			
faultlog.txt file 11-2	scenarios 4-13			
excluding networks from auto initiation 7-3	CPP 4-11			
export operation 9-5	custom 4-17			
	defining filters and rules 4-15			
	Integrity Server 1-19, 4-11			
F	notifications during negotiations 4-18			
fallback mode 11-9	personal firewall			

enforcement on remote PC 1-19, 4-11	VPN attributes 3-15
requiring 1-17, 4-10	group policy, default 3-11
stateful on VPN Client 1-18, 4-10	GroupPwd parameter (.pcf file) 5-26
Sygate Personal Firewall 1-19, 4-11	GUI parameters 5-13
Sygate Personal Firewall Pro 1-19, 4-11	
Sygate Security Agent 1-19, 4-11	11
Zone Alarm Firewall 1-19, 4-11	Н
Zone Alarm Pro Firewall 1-19, 4-11	hash 9-2
ForceNetlogin parameter (.pfc file) 5-31	help files, Japanese 1-5
formats	HKEY_LOCAL_MACHINE 11-9
data 1-xvii	Host parameter (.pcf file) 5-25
FQDN (fully qualified domain name) 9-2	
fragmentation	
preventing 11-5	l
	icons
 G	connected.ico 10-3
O	disconnecting.ico 10-3
general attributes, tunnel group 3-2	unconnected.ico 10-3
general parameters, tunnel group 3-2	ID method, determining 1-15
general tunnel-group connection parameters 3-2	IKE
global profile	identification methods 1-15
creating 5-2	keepalives 1-16
graphics, rebranding 10-1	keepalive setting, tunnel group 3-3
GroupName parameter (.pcf file) 5-26	IKE, configuring 1-13
group policy	IKE proposals
address pools 3-24	activating 4-5
attributes 3-14	list 11-13
backup server attributes 3-23	phase 2 11-16
client access rules 3-27	import operation 9-5
configuring 3-14	incompatible ginas
default domain name for tunneled packets 3-21	adding 11-9
definition 3-11	fallback mode 11-9
domain attributes 3-21	start before logon feature 11-8
firewall policy 3-25	IncompatibleGinas parameter (vpnclient.ini file) 5-5
internal, configuring 3-14	initializing VA
IPSec over UDP attributes 3-19	changing method 5-8
security attributes 3-17	Installation
split tunneling attributes 3-20	MSI requirements 12-1
split-tunneling domains 3-22	

logging during installation 12-3	Organization 10-1
silent install 10-7	organizational unit field in certificate 4-5
msiexec command 10-7	organization logo
MSI transform	logo.png file 10-1
customizing VPN Client 10-3	
installing 10-7	P
MSLogonType parameter (.pcf file) 5-28	P
MTU setting	parameters
affects of 11-5	global
changing 11-5	table 5-5
mutual authentication 5-25	peer timeout (.pcf file) 5-29
mutual group authentication 1-13, 4-26	profile (.pcf)
	authentication 5-27
 N	AuthType 5-25
TV	BackupServer 5-28
NAT-T, enabling IPsec 1-14	certificate parameters 5-29
NAT Transparency (NAT-T)	Description 5-25
configuring on VPN Concentrator 4-22	DHGroup 5-30
Net login	EnableISPConnect 5-26
forcing 5-31	EnableLocalLAN 5-29
Netlogin parameters 5-12	EnableMSLogon 5-28
Network Ice firewall 3-26	EnableNat 5-28
new/modify profile dialog	EnableSplitDNS 5-31
profile_logo.png 10-2	encGroupPwd 5-26
new_update_config.ini file	ForceNetlogin 5-31
parameters (table) 6-5	GroupName 5-26
new connection entries	GroupPwd 5-26
distributing 6-6	Host 5-25
notifications	ISPCommand 5-27
displaying 8-5	ISPConnect 5-26
firewalls 4-18	ISPConnectType 5-26
upgrade 4-19, 6-1	MSLogonType 5-28
notify command 8-5	NTDomain 5-27
NTDomain parameter (.pfc file) 5-27	PeerTimeout 5-29
	RadiusSDI 5-30
0	SaveUserPassword 5-27
O	SDIUseHardwareToken 5-30
operations for certificate management 9-4	SendCertChain 5-30
	TCPTunnelingPort 5-28

TunnelingMode 5-28	pcf files
UseLegacyIKEPort 5-31	creating 5-22
VerifyCertDN 5-30	distributing with VPN Client software 5-33
read only 5-2	parameters 5-25
vpnclient.ini	sample 5-24
AppendOriginalSuffixOption 5-21	PeerTimeout parameter (.pcf file) 5-29
ApplicationLauncher 5-11	personal firewall 1-17
AutoInitiationEnable 5-6	personal firewalls
AutoInitiationList 5-7	configuring for VPN Client
AutoInitiationRetrylLimit 5-7	VPN Concentrator 1-17, 4-9
AutoInitiationRetryType 5-7	phase 2 IKE proposals 11-16
certificate enrollment 5-9	PKIs
ConnectOnOpen	supported 4-9, 5-14
configuring 5-8	Portable Network Graphic (PNG) files
DialerDisconnect 5-6	list 10-1
DNS 5-11	preconfigured connection entry
EnableLog 5-6	distributing 5-33
EntrustIni 5-5	preconfigured files 10-8
GUI 5-13	preconfiguring VPN Clients for remote users 5-1
IncompatibleGinas 5-5	pre-shared key authentication
log class 5-9	certificate authentication 5-25
LogLevel 5-9	primary DNS suffix 5-19
MissingGroupDialog 5-5	printing by name on local LAN 1-21, 4-21
Netlogin 5-12	profile
RADIUS SDI 5-11	connection entry 5-22
RunAtLogon 5-5	creating user 4-4
StatefulFirewall 5-6	directory 5-2
StatefulFirewallAllowICMP 5-6	Entrust 1-10, 4-23
table 5-5	file format 5-2
vpnclient command 8-7	global 5-2
vpnclient stat command	features controlled 5-2
firewall 8-7	parameters 5-4
repeat 8-7	sample 5-3
reset 8-7	profile_logo.png
route 8-7	new/modify profile dialog 10-2
traffic 8-7	profiles
tunneling 8-7	distributing 6-6
password_logo.png	programmer notes
Xauth dialog 10-2	testing a connection 11-9

1	
proposals	S
IKE 4-5, 11-13	SA
phase 2 IKE 11-16	
Public Key Infrastructure	adding 4-5
see PKIs	sample files
	.pcf file 5-24
Q	vpnclient.ini 5-3
	SaveUserPassword parameter (.pfc file) 5-27
quick configuration 1-7	SDIUseHardwareToken parameter (.pfc file) 5-30
	Security Agent, Cisco 3-26
R	security attributes, group policy 3-17
	SendCertChain parameter 5-30
RADIUS SDI authentication	SetMTU utility 11-5
configuring 5-21	launching silently 10-7
RadiusSDI parameter (.pfc file) 5-30	SHA 11-13
RADIUS SDI parameters 5-11	silent install 10-1
read-only parameters 5-2	MSI 10-7
rebootless client upgrade 1-4	silent installation 10-7
rebranding the Client 10-1	smart card authentication 1-12
registry	software updates, getting 6-4
testing a connection 11-9	splash screen
related documentation 1-xiv	splash_screen.png
remote access	splash_screen.png 10-1
IPSec tunnel group, configuring 3-5	splash screen, changing 10-1
tunnel group, configuring default 3-4	Split DNS
Remote Firewall	enabling 5-31
scenario 4-13	split tunneling
requirements, system 1-3	group policy 3-20
resetting counts 8-7	group policy, domains 3-22
root certificates 9-2	Start Before Logon
routing information 8-7	support 1-3
RSA 11-13	start before logon
rules	gina files 11-8
defining for CPP 4-15	starting a connection 8-2
RunAtLogon parameter (vpnclient.ini) 5-5	stateful firewall (always on) 1-18, 4-10
Rum REogon parameter (vpnenencim)	StatefulFirewallAllowICMP parameter (vpnclient.ini) 5-6
	StatefulFirewall parameter (vpnclient.ini) 5-6
	status information

generating 8-7	U
Sygate Personal Firewall 3-26	O .
firewall on remote PC 1-19, 4-11	UniCERT 4-9, 5-14
Sygate Personal Firewall Pro	updated VPN Client software, getting 6-4
firewall on remote PC 1-19, 4-11	updating VPN Client software
Sygate Security Agent	all client types 6-1
firewall on remote PC 1-19, 4-11	automatically (Windows 2000 and Windows XP) 6-2
system information	Linux 6-2
Windows 98 11-1	MAC OS X 6-2
Windows NT 11-3	Solaris 6-2
system requirements 1-3	upgrade, rebootless client 1-4
system security	upgrade notifications
protecting 5-24	configured on VPN Concentrator 4-19, 6-1
	UseLegacyIKEPort parameter (.pfc file) 5-31
 T	user certificates 9-1
1	user profiles
TCP, enabling IPsec 1-14	certificate
TCPTunnelingPort parameter (.pcf file) 5-28	keywords 9-1
testing a connection 11-9	creating for distribution 5-22
traffic information 8-7	creating in VPN Concentrator 4-4
transform 10-3	location 5-2, 5-22
installing 10-7	
troubleshooting	V
connectivity application 11-5	V
generating information 11-1	VAenableAlt 5-8
TunnelEstablished parameter in registry 11-9	VerifyCertDN parameter (.pfc file) 5-30
tunnel group	verifying an auto initiation configuration 7-5, 8-5
configuring 3-4	verify operation 9-5
creating 3-5	view operation 9-4
default, remote access, configuring 3-4	virtual adapter
general parameters 3-2	method of initializing 5-8
IPSec parameters 3-3	VPN
name and type 3-5	address pool, configuring (group-policy) 3-24
remote-access, configuring 3-5	VPN attributes, group policy 3-15
tunnel-group	VPN Client
general attributes 3-2	applications 1-xi
tunnel-group ISAKMP/IKE keepalive settings 3-3	configuring 5-1
tunneling information 8-7	configuring, general 1-7
TunnelingMode parameter (.pcf file) 5-28	using 1-6

vpnclient.ini file		
file format 5-2		
sample 5-3		
vpnclient_en.msi command 12-2		
vpnclient commands		
disconnect 8-6		
displaying a list 8-1		
notify 8-5		
stat 8-7		
firewall 8-7		
repeat 8-7		
reset 8-7		
route 8-7		
traffic 8-7		
tunnel 8-7		
verify autoinitconfig 8-5		
VPN Client for Linux firewall, configuring 1-20		
VPN Client GUI, customizing for Mac OS X 10-8		
VPN Concentrator		
configuring personal firewalls for VPN Client 1-17, 4-9		
creating user profiles 4-4		
W		
VV		
welcome message, group policy 3-19		
Windows 98		
generating system information 11-3		
shut down problem 11-5		
Windows installer (MSI) 12-1		
Windows NT or Windows 2000		
generating system information 11-3		
WINMSD utility		
Windows NT or Windows 2000 11-3		
X		
Xauth dialog		
password_logo.png 10-2		

Ζ

Zone Alarm Firewall
firewall on remote PC 1-19, 4-11
Zone Alarm Pro Firewall
firewall on remote PC 1-19, 4-11
Zone Labs firewall 1-18
Zone Labs firewalls 3-26

Index